+357 96 030922
info@marketpublishers.com

The Quantum Cybersecurity Market 2027-2037

https://marketpublishers.com/r/Q0992327FBF4EN.html
Date: October 2026
Pages: 398
Price: US$ 1,650.00 (Single User License)
ID: Q0992327FBF4EN

Abstracts

Quantum cybersecurity covers the technologies and services that protect data, communications and digital identities against attack by cryptographically relevant quantum computers (CRQCs). A machine of this kind running Shor's algorithm would break the RSA and elliptic-curve public-key cryptography that secures almost every digital transaction, network session, software update and identity system in use today. The threat is already live, because adversaries can harvest encrypted traffic now and decrypt it once quantum capability arrives. Data with a confidentiality life of ten years or more is therefore exposed today.

In 2026 the market moved from preparation to compliance. NIST finalised the post-quantum standards ML-KEM, ML-DSA and SLH-DSA in 2024, and FN-DSA and HQC are close behind. The June 2026 US executive order (EO 14412) and OMB memorandum M-26-15 require quantum-resistant key establishment for high-value federal systems by the end of 2030 and signatures by 2031. A FAR rule is set to extend the 2030 deadline to federal contractors. CNSA 2.0 requires new US national security system acquisitions to be quantum-safe from January 2027. The EU coordinated roadmap, the UK NCSC timeline, Germany's BSI, France's ANSSI, India, Australia and the G7 financial sector have set comparable milestones. Readiness lags far behind: in October 2026 the US GAO found that only one of 24 major federal agencies had completed its cryptographic inventory.

The market spans six areas:

post-quantum cryptography (PQC) software, libraries and IP;

PQC-enabled hardware such as HSMs, secure elements and silicon;

cryptographic discovery and crypto-agility platforms;

+357 96 030922
info@marketpublishers.com

quantum key distribution (QKD);

quantum random number generators (QRNG);

quantum-safe migration and managed services.

The Global Quantum Cybersecurity Market 2027–2037 is an in-depth analysis of the market for quantum-safe security products and services, with forecasts from 2027 to 2037 and information current to October 2026. It sets out how binding deadlines in the United States, Europe and Asia-Pacific are turning post-quantum migration into funded programmes. It sizes the opportunity for vendors, operators, integrators and investors.

The report provides ten-year forecasts in two ways. The first is by product segment: PQC software and IP, PQC-enabled hardware, discovery and crypto-agility platforms, QKD and QRNG. The second is a total addressable market for products and migration services split by cryptographic approach: lattice-based PQC, hash-based signatures, code-based and other PQC, symmetric and key-distribution architectures, QKD and QRNG. Forecasts are also broken down by end-use market, region, device type, QKD system type and service type, with three growth scenarios. The report also estimates the installed base of routers, switches, firewalls and SD-WAN by major vendor, and how quickly it becomes PQC-capable through hardware refresh. A comprehensive company profiles section covers 72 companies.

Report contents include:

The quantum threat and Q-Day timeline: CRQC resource estimates, hardware roadmaps, harvest-now-decrypt-later exposure and data shelf-life by sector.

Policy, regulation and standards: EO 14412, OMB M-26-15, CNSA 2.0, the GAO’s October 2026 findings, the Treasury Quantum-Readiness Task Force, the G7 roadmap, EU, UK, German, French, Asia-Pacific mandates, and NIST, IETF, ETSI and ISO standards.

Post-quantum cryptography technology: algorithms, performance, hybrid TLS and IPsec, PKI, code signing, embedded systems and open-source libraries.

Cryptographic discovery, CBOM and crypto-agility platforms.

+357 96 030922
info@marketpublishers.com

PQC hardware: HSMs, secure elements, TPMs, IP cores and network encryptors.

Quantum key distribution: protocols, trusted-node and satellite networks, certification and the vendor landscape.

Quantum random number generation: entropy sources, form factors, certification and applications.

Quantum-safe networks: telecom operators, national backbones, hybrid PQC/QKD architectures and convergence with Zero Trust.

Network infrastructure installed base by vendor and the quantum-safe refresh cycle.

Migration services and managed quantum-safe security, including the federal contractor requirements.

End-use markets: government and defence, financial services, telecoms, cloud, critical infrastructure, healthcare, automotive and IoT, and digital assets.

Competitive landscape, M&A, venture funding and public companies.

Drivers, restraints, SWOT, technology readiness and opportunity assessment.

Ten-year market forecasts with 110+ tables and 85 figures.

Regional analysis across North America, Europe, Asia-Pacific, the Middle East & Africa and Latin America.

72 company profiles including 01 Quantum (formerly 01 Communique), Accenture, Aliro, Amazon Web Services, American Binary, Apple, Arqit Quantum, BT Group, BTQ Technologies, Cisco, Cloudflare, Crypta Labs, Crypto4A Technologies, CryptoNext Security, Crypto Quantique, DigiCert, Eclypses, Encryption Consulting, Entrust, evolutionQ, Fortanix, Google, HEQA Security (formerly QuantLR), IBM, ID Quantique, Infineon Technologies, IonQ, KEEQuant, KETS Quantum Security, Keyfactor, Lattice Semiconductor, LuxQuanta, Microsoft, Numana, Nu Quantum, NXP Semiconductors, Palo Alto

+357 96 030922
info@marketpublishers.com

Networks, Patero, Post-Quantum (PQ Solutions), PQSecure Technologies, PQShield and more.....

+357 96 030922
info@marketpublishers.com

Contents

1. RESEARCH SCOPE AND METHODOLOGY

1.1 Report Scope and Objectives
1.2 Research Approach
1.3 Market Definition and Segmentation
1.4 Forecasting Model
1.5 Assumptions and Limitations
1.6 Terms and Definitions

2. EXECUTIVE SUMMARY

2.1 The Quantum Threat in Brief
2.2 2026: The Year Deadlines Became Law
2.3 Market Definition and Scope
2.4 Headline Market Forecast
2.5 Ten-Year TAM by Cryptographic Approach
2.6 The Network Installed Base
2.7 Segment Highlights
2.8 End-Use Markets
2.9 Drivers and Restraints
2.10 Competitive and Investment Highlights
2.11 Regional Summary
2.12 Principal Findings and Strategic Recommendations

3. INTRODUCTION TO QUANTUM CYBERSECURITY

3.1 What Is Quantum Cybersecurity?
3.2 Classical Public-Key Cryptography and Its Vulnerabilities
3.3 Shor's and Grover's Algorithms
3.4 Symmetric Versus Public-Key Cryptography in a Quantum World
3.5 PQC, QKD, QRNG and Hybrid Approaches Compared
3.6 The Quantum-Safe Security Stack and Market Map
3.7 Market Drivers in Brief
3.8 Report Scope, Segmentation and Methodology
3.9 Cryptographic Terminology

4. THE QUANTUM THREAT AND Q-DAY TIMELINE

+357 96 030922
info@marketpublishers.com

4.1 Cryptographically Relevant Quantum Computers
4.2 Falling Resource Estimates
4.3 Quantum Hardware Roadmaps
4.4 Q-Day Estimates and Uncertainty
4.5 The Harvest-Now-Decrypt-Later Threat
4.6 Mosca's Inequality and Data Shelf-Life
4.7 Digital Assets and Blockchain Exposure
4.8 Classical Risks to the New Algorithms
4.9 Adversaries, Geopolitics and the Covert-Capability Problem
4.10 Strategic Implications

5. POLICY, REGULATION AND STANDARDS

5.1 The Shift from Guidance to Mandate
5.2 United States: Federal Civilian Systems
  5.2.1 Executive Order 14412 (June 2026)
  5.2.2 OMB Memorandum M-26-15
  5.2.3 The Contractor Cascade
  5.2.4 CISA Product Categories (January 2026)
5.3 United States: National Security Systems
5.4 NIST Standards and the US Technical Baseline
5.5 The October 2026 GAO Audit
5.6 US Financial Sector Initiatives
5.7 International Financial-Sector Bodies and Sector Regulators
5.8 European Union
5.9 European National Regimes
5.10 United Kingdom
5.11 Americas outside the United States
5.12 Asia-Pacific
5.13 Global Mandate and Deadline Matrix
5.14 Standards Bodies and Protocol Standards
5.15 The QKD Policy Divide
5.16 Policy Outlook 2027–2030

6. POST-QUANTUM CRYPTOGRAPHY TECHNOLOGY

6.1 Algorithm Families
6.2 The NIST Standards

+357 96 030922
info@marketpublishers.com

6.3 Performance and Key-Size Implications
6.4 Hybrid Key Exchange
6.5 Protocol Integration
6.6 Quantum-Safe PKI and Certificates
6.7 Code Signing, Firmware and Roots of Trust
6.8 Embedded, IoT and Constrained Devices
6.9 Side-Channel and Implementation Security
6.10 Open-Source Libraries and Implementations
6.11 Adoption Metrics

7. CRYPTOGRAPHIC DISCOVERY, INVENTORY AND CRYPTO-AGILITY

7.1 Why Inventory Is the Bottleneck
7.2 The Cryptographic Bill of Materials
7.3 Discovery Techniques
7.4 From Inventory to Remediation
7.5 Certificate Lifecycle Management and Quantum-Safe PKI
7.6 Crypto-Agility
7.7 Cryptographic Posture Management Platforms
7.8 Vendor Landscape
7.9 Buyer Criteria
7.10 Segment Forecast 2027–2037
7.11 Strategic Implications

8. PQC HARDWARE: HSMS, SECURE ELEMENTS AND SILICON

8.1 Why Hardware Sets the Pace of Migration
8.2 Hardware Security Modules
8.3 Secure Elements, TPMs and Smart Cards
8.4 PQC IP Cores, Accelerators and Microcontrollers
8.5 Network Encryptors and VPN Appliances
8.6 Implementation Security and Certification
8.7 PQC Hardware Forecast 2027–2037
8.8 PQC Software, Libraries and IP Forecast 2027–2037
8.9 Strategic Implications

9. QUANTUM KEY DISTRIBUTION

9.1 Principles of Quantum Key Distribution

+357 96 030922
info@marketpublishers.com

9.2 QKD Protocol Families
9.3 Trusted-Node Networks
9.4 Satellite and Free-Space QKD
9.5 Integration with Key Management and Encryption Infrastructure
9.6 Certification and Standardisation
9.7 Government Positions: Support versus Scepticism
9.8 Cost Structure and Economics
9.9 Vendor Landscape
9.10 QKD Market Forecast 2027–2037
9.11 Outlook and Strategic Implications

10. QUANTUM RANDOM NUMBER GENERATION

10.1 Why Randomness Matters for Quantum-Safe Security
10.2 Entropy Sources
10.3 Form Factors and Delivery Models
10.4 Certification and Standards
10.5 Applications
  10.5.1 Mobile Devices
  10.5.2 Hardware Security Modules and Key Management
  10.5.3 IoT, Industrial and Automotive
  10.5.4 Gaming, Lotteries and Simulation
  10.5.5 Finance, Blockchain and Certified Randomness
  10.5.6 Government and Defence
10.6 Integration Patterns with Post-Quantum Cryptography
10.7 Vendor Landscape
10.8 QRNG Market Forecast 2027–2037
10.9 Outlook and Strategic Implications

11. QUANTUM-SAFE NETWORKS AND COMMUNICATIONS INFRASTRUCTURE

11.1 Telecom Operators as Quantum-Safe Service Providers
11.2 National Quantum Communication Backbones
11.3 Hybrid PQC and QKD Architectures
11.4 Convergence with Zero Trust and Network Security
11.5 5G, 6G and Mobile Network Security
11.6 Quantum Networking and the Road to a Quantum Internet
11.7 Market Implications

+357 96 030922
info@marketpublishers.com

12. NETWORK INFRASTRUCTURE INSTALLED BASE AND THE QUANTUM-SAFE REFRESH

12.1 Why Network Equipment Is the Quantum-Safe Chokepoint
12.2 Methodology and Definitions
12.3 The Installed Base by Equipment Class
12.4 Installed Base by Vendor
  12.4.1 Routers
  12.4.2 Ethernet Switches
  12.4.3 Firewalls and Security Appliances
  12.4.4 SD-WAN and SASE Edges
  12.4.5 Combined View by Vendor
12.5 Vendor PQC Roadmaps
12.6 Refresh Cycles and the PQC-Capable Trajectory
12.7 Implications for the Quantum Cybersecurity Market

13. MIGRATION SERVICES AND MANAGED QUANTUM-SAFE SECURITY

13.1 Why Services Dominate the Market
13.2 Services Market Structure
13.3 Services Forecast 2027–2037
13.4 Sector Patterns in Services Demand
13.5 The US Contractor Cascade
13.6 Provider Landscape
13.7 Engagement and Pricing Models
13.8 Managed Quantum-Safe Services
13.9 Constraints on Services Growth
13.10 Strategic Implications

14. END-USE MARKETS

14.1 Overview of End-User Demand
14.2 Government and Defence
14.3 Banking, Financial Services and Insurance
14.4 Telecommunications
14.5 Cloud, Hyperscale and IT Services
14.6 Energy, Utilities and Critical Infrastructure
14.7 Healthcare and Life Sciences
14.8 Automotive, IoT and Manufacturing

+357 96 030922
info@marketpublishers.com

14.9 Digital Assets and Blockchain
14.10 Other Enterprise
14.11 Migration Timing by Sector
14.12 End-User Opportunity Assessment

15. COMPETITIVE LANDSCAPE, INVESTMENT AND M&A

15.1 Market Structure
15.2 Mergers and Acquisitions
15.3 Venture and Growth Investment
15.4 Publicly Listed Quantum Cybersecurity Companies
15.5 Business Models
15.6 Competitive Positioning
15.7 Indicative Vendor Leadership by Segment
15.8 Partnerships and Ecosystems
15.9 Strategic Outlook

16. MARKET DYNAMICS AND OPPORTUNITY ASSESSMENT

16.1 Market Drivers
16.2 Market Restraints
16.3 Impact Assessment of Drivers and Restraints
16.4 SWOT Analysis
16.5 Porter's Five Forces
16.6 Technology Readiness Assessment
16.7 Per-Segment SWOT
16.8 Opportunity Ranking
16.9 Pricing and Cost Dynamics
16.10 Leading Indicators to Monitor
16.11 Key Challenges
16.12 Recommendations

17. MARKET FORECASTS 2027–2037

17.1 Forecast Definitions and Assumptions
17.2 Total Market Size 2027–2037
17.3 Core Technology Market by Segment
  17.3.1 PQC Software, Libraries and IP
  17.3.2 PQC-Enabled Hardware

+357 96 030922
info@marketpublishers.com

17.3.3 Cryptographic Discovery and Crypto-Agility Platforms
17.3.4 Quantum Key Distribution Systems
17.3.5 Quantum Random Number Generators
17.4 Migration and Managed Services
17.5 Forecast by Technology Approach
17.6 Ten-Year TAM by Cryptographic Approach
17.6.1 Approach Definitions and Allocation Method
17.6.2 Products TAM by Approach
17.6.3 Migration Services TAM by Approach
17.6.4 Total TAM by Approach
17.7 Forecast by End-User Sector
17.8 Forecast by Region
17.9 Growth Scenarios

18. REGIONAL ANALYSIS

18.1 North America
18.1.1 United States
18.1.2 Canada
18.2 Europe
18.2.1 European Union
18.2.2 United Kingdom
18.2.3 Germany
18.2.4 France
18.2.5 Netherlands, Switzerland, Nordics, Spain and Italy
18.3 Asia-Pacific
18.3.1 China
18.3.2 Japan
18.3.3 South Korea
18.3.4 India
18.3.5 Singapore, Australia and Taiwan
18.4 Middle East and Africa
18.5 Latin America
18.6 Regional Summary

19. COMPANY PROFILES (72 COMPANY PROFILES)

20. REFERENCES

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

Table 1. Report identity card: scope, segmentation and coverage.
Table 2. Principal model inputs and evidence sources.
Table 3. Terms and definitions used in this report.
Table 4. Core quantum cybersecurity technology market by segment, 2027–2037 (millions USD).
Table 5. Total quantum cybersecurity market including migration and managed services, 2027–2037 (millions USD).
Table 6. Total TAM (products and migration services) by cryptographic approach, 2027–2037 (millions USD).
Table 7. Core quantum cybersecurity technology market by region, 2027–2037 (millions USD).
Table 8. Exposure of widely deployed cryptographic algorithms to quantum attack.
Table 9. Comparison of quantum-safe security approaches.
Table 10. Principal drivers of the quantum cybersecurity market and their timing.
Table 11. Market segmentation used in this report and headline values (millions USD).
Table 12. Key cryptographic and quantum security terms.
Table 13. Selected published resource estimates for breaking public-key cryptography.
Table 14. Selected quantum computing hardware roadmaps relevant to the CRQC threshold.
Table 15. Reference Q-Day estimates and planning assumptions, 2026.
Table 16. Indicative data confidentiality requirements by sector and implied urgency.
Table 17. Quantum exposure of major blockchain ecosystems.
Table 18. Executive Order 14412 and OMB M-26-15 — principal US federal civilian milestones.
Table 19. NSA CNSA 2.0 transition timeline by equipment category.
Table 20. NIST post-quantum standards and related publications, status at October 2026.
Table 21. GAO-27-108740 — key findings on federal PQC preparation.
Table 22. Sector regulators and industry bodies shaping quantum-safe requirements.
Table 23. Global quantum-safe mandate and deadline matrix, October 2026.
Table 24. Principal standards bodies and quantum-safe standards.
Table 25. National policy stances on QKD.
Table 26. PQC algorithm families — characteristics and trade-offs.
Table 27. NIST post-quantum cryptography standards and status, October 2026.
Table 28. Key, ciphertext and signature sizes and relative performance.

+357 96 030922
info@marketpublishers.com

Table 29. Post-quantum integration status of major protocols, October 2026.
Table 30. Major PQC cryptographic libraries and their status.
Table 31. Selected platform post-quantum milestones and stated migration targets.
Table 32. Core elements of a cryptographic bill of materials (CBOM) and their migration relevance.
Table 33. Comparison of cryptographic discovery techniques.
Table 34. Quantum-safe PKI design choices and market implications.
Table 35. Crypto-agility maturity levels — characteristics and typical tooling.
Table 36. Cryptographic discovery, CLM and crypto-agility vendor landscape.
Table 37. Buyer evaluation criteria for discovery and crypto-agility platforms.
Table 38. Cryptographic discovery and crypto-agility platform market by sub-segment 2027–2037 (millions USD).
Table 39. Typical hardware replacement cycles and PQC migration implications.
Table 40. Leading HSM vendors and PQC capabilities (late 2026).
Table 41. PQC secure elements, TPMs and secure microcontrollers — selected products.
Table 42. PQC hardware IP and accelerator suppliers.
Table 43. PQC-enabled hardware market by device category 2027–2037 (millions USD).
Table 44. PQC software, libraries and IP market by category 2027–2037 (millions USD).
Table 45. Principal QKD protocols — characteristics, indicative performance and commercial status, 2026.
Table 46. QKD network architectures compared.
Table 47. Selected satellite QKD missions and programmes.
Table 48. Key QKD standards and certification frameworks.
Table 49. National positions on QKD, 2026.
Table 50. Indicative QKD deployment costs, 2026 vs. 2032 (US$, Future Markets estimates).
Table 51. Selected QKD vendors and their positioning, 2026.
Table 52. Global QKD systems market by technology type, 2027–2037 (millions USD).
Table 53. Global QKD systems market by region, 2027–2037 (millions USD).
Table 54. QRNG entropy sources compared.
Table 55. QRNG form factors and delivery models.
Table 56. Certification frameworks relevant to QRNGs.
Table 57. Selected QRNG suppliers and offerings, 2026.
Table 58. Global QRNG market by form factor and delivery model, 2027–2037 (millions USD).
Table 59. Indicative embedded QRNG chip shipments and average selling price, 2027–2037 (Future Markets estimates).

+357 96 030922
info@marketpublishers.com

Table 60. Selected telecom operator quantum-safe network initiatives, 2022–2026.
Table 61. Telecommunications sector spend on core quantum cybersecurity technologies, 2027–2037 (millions USD).
Table 62. Major national and regional quantum communication network programmes, 2026.
Table 63. Quantum-safe network protection options by link type.
Table 64. Selected quantum networking companies and their focus.
Table 65. Quantum-safe network infrastructure — demand drivers and constraints.
Table 66. Estimated installed base of network infrastructure by equipment class, 2026.
Table 67. Estimated router installed base by vendor, 2026.
Table 68. Estimated Ethernet switch installed base by vendor, 2026.
Table 69. Estimated firewall and security-appliance installed base by vendor, 2026.
Table 70. Estimated SD-WAN edge installed base by vendor, 2026.
Table 71. Combined installed base of routers, switches, firewalls and SD-WAN edges by major vendor, 2026.
Table 72. Network vendor PQC capabilities and roadmaps, October 2026.
Table 73. Typical service lives and quantum-safe upgrade paths by equipment class.
Table 74. PQC-capable share of the installed base by equipment class, 2026–2037 (Future Markets estimates).
Table 75. PQC-capable versus classical-only network devices in service, 2026–2037 (millions of units).
Table 76. Quantum-safe services categories — definition and characteristics.
Table 77. Quantum-safe migration and managed services market by category 2027–2037 (millions USD).
Table 78. Quantum-safe services market by region 2027–2037 (millions USD).
Table 79. Services demand profile by end-user sector.
Table 80. Key policy drivers of quantum-safe services demand.
Table 81. Selected quantum-safe services providers and positioning.
Table 82. Quantum-safe services engagement and pricing models (indicative, 2026).
Table 83. Core quantum cybersecurity technology market by end user, 2027–2037 (millions USD).
Table 84. End-user groups — demand triggers, buying behaviour and preferred technologies.
Table 85. Indicative core technology spending mix by end user, 2030 (% of each end user's spend).
Table 86. Sector migration milestones, regulatory anchors and peak spending windows.
Table 87. End-user opportunity ranking and recommended vendor posture.
Table 88. Quantum cybersecurity participant groups — role, revenue model and competitive advantage.

+357 96 030922
info@marketpublishers.com

Table 89. Selected M&A transactions relevant to quantum cybersecurity, 2022–October 2026.
Table 90. Selected funding rounds in quantum cybersecurity, 2024–October 2026.
Table 91. Selected listed companies with quantum cybersecurity activities (as of October 2026).
Table 92. Business models in quantum cybersecurity.
Table 93. Indicative leaders and market concentration by segment, 2026–2027.
Table 94. Representative partnership types in quantum cybersecurity.
Table 95. Driver and restraint impact scores by period (1 = low, 5 = high).
Table 96. Porter's five forces analysis of the quantum cybersecurity market.
Table 97. Technology readiness of quantum cybersecurity market elements, 2026.
Table 98. SWOT summary by core technology segment.
Table 99. Opportunity ranking for vendors, 2027–2037.
Table 100. Indicative price points for quantum cybersecurity products, 2026–2027 (Future Markets estimates).
Table 101. Leading indicators and their implications for market trajectory.
Table 102. Market definition and segmentation used in this report.
Table 103. Key forecast assumptions.
Table 104. Global quantum cybersecurity market — core technology and services 2027–2037 (millions USD).
Table 105. Year-on-year growth of the quantum cybersecurity market, 2028–2037 (%).
Table 106. Core quantum cybersecurity technology market by segment 2027–2037 (millions USD).
Table 107. Core quantum cybersecurity market — segment share 2027, 2032 and 2037 (%).
Table 108. Segment summary — size, growth and principal demand drivers.
Table 109. PQC-enabled hardware market by device type 2027–2037 (millions USD).
Table 110. QKD systems market by type 2027–2037 (millions USD).
Table 111. QRNG market by form factor 2027–2037 (millions USD).
Table 112. Quantum-safe migration and managed services market by category 2027–2037 (millions USD).
Table 113. Core quantum cybersecurity market by technology approach 2027–2037 (millions USD).
Table 114. Cryptographic approaches used to segment the TAM.
Table 115. Products TAM by cryptographic approach, 2027–2037 (millions USD).
Table 116. Quantum-safe migration and managed services TAM by cryptographic approach, 2027–2037 (millions USD).
Table 117. Total TAM (products and migration services) by cryptographic approach, annual 2027–2037 (millions USD).

+357 96 030922
info@marketpublishers.com

Table 118. Total TAM by cryptographic approach — products, services, share and growth.
Table 119. Cumulative TAM by cryptographic approach, 2027–2037 (millions USD).
Table 120. Core quantum cybersecurity market by end-user sector 2027–2037 (millions USD).
Table 121. Core quantum cybersecurity market by region 2027–2037 (millions USD).
Table 122. Scenario assumptions.
Table 123. Total quantum cybersecurity market (incl. services) — growth scenarios 2027–2037 (millions USD).
Table 124. Core quantum cybersecurity market by region 2027–2037 (millions USD).
Table 125. QKD systems market by region 2027–2037 (millions USD).
Table 126. Regional market characteristics summary.
Table 127. Country-level quantum cybersecurity readiness — policy deadlines, QKD programmes and key vendors.

+357 96 030922
info@marketpublishers.com

List Of Figures

LIST OF FIGURES

Figure 1. Core quantum cybersecurity technology market by segment, 2027–2037 (millions USD).
Figure 2. Total quantum cybersecurity market: core technology and migration and managed services, 2027–2037 (millions USD).
Figure 3. Total TAM by cryptographic approach, 2027–2037 (millions USD).
Figure 4. Quantum cybersecurity market drivers and restraints.
Figure 5. Core quantum cybersecurity technology market by region, 2037.
Figure 6. How a quantum computer breaks public-key cryptography.
Figure 7. PQC, QKD and QRNG: three quantum-era security approaches.
Figure 8. The quantum-safe security stack: six market segments.
Figure 9. Core quantum cybersecurity technology market by segment, 2037 (% of value).
Figure 10. Estimated physical qubits required to break RSA-2048, 2012–2026 (log scale).
Figure 11. Indicative quantum hardware milestones and cryptographic deadlines, 2024–2036.
Figure 12. Share of surveyed experts assessing ?50% likelihood of an RSA-2048-breaking quantum computer, by horizon.
Figure 13. Harvest now, decrypt later: why migration cannot wait for Q-Day.
Figure 14. Mosca's inequality: when x + y exceeds z, data is exposed.
Figure 15. Quantum-safe standardisation and mandate timeline, 2016–2037.
Figure 16. US federal agency PQC readiness at the end of the GAO audit period (24 CFO Act agencies).
Figure 17. Comparison of national quantum-safe migration deadlines.
Figure 18. The four families of post-quantum cryptography.
Figure 19. Key and signature sizes: classical versus post-quantum algorithms (bytes, log scale).
Figure 20. Hybrid post-quantum key exchange in TLS 1.3 (X25519MLKEM768).
Figure 21. Share of human HTTPS traffic to Cloudflare protected by post-quantum key agreement.
Figure 22. The six layers of cryptographic discovery.
Figure 23. The continuous cryptographic inventory-to-remediation loop.
Figure 24. Crypto-agility maturity model.
Figure 25. Cryptographic discovery and crypto-agility platform market by sub-segment 2027–2037 (millions USD).

+357 96 030922
info@marketpublishers.com

Figure 26. Typical service life of devices shipped in 2027 versus 2030 and 2035 cryptographic deadlines.
Figure 27. PQC-enabled hardware market by device category 2027–2037 (millions USD).
Figure 28. PQC-enabled hardware market by device category, 2037.
Figure 29. PQC software, libraries and IP market by category 2027–2037 (millions USD).
Figure 30. Indicative secret key rate versus fibre distance by QKD protocol family.
Figure 31. Trusted-node QKD relay: hop-by-hop key generation and XOR forwarding.
Figure 32. QKD system and network integration stack.
Figure 33. Global QKD systems market by technology type, 2027–2037 (millions USD).
Figure 34. Global QKD systems market by region, 2027–2037 (millions USD).
Figure 35. Regional share of the QKD systems market, 2037.
Figure 36. The QRNG entropy chain: from quantum source to cryptographic key.
Figure 37. Global QRNG market by form factor and delivery model, 2027–2037 (millions USD).
Figure 38. QRNG market share by form factor and delivery model, 2037.
Figure 39. Indicative annual shipments of embedded QRNG chips, 2027–2037 (millions of units).
Figure 40. Indicative scale of operational or announced QKD fibre networks by programme, 2026 (km).
Figure 41. Hybrid PQC–QKD architecture for high-assurance data-centre interconnect.
Figure 42. Stages in the evolution from QKD networks to a quantum internet.
Figure 43. Quantum-safe and quantum networking deployment timeline, 2016–2037.
Figure 44. Estimated installed base of network infrastructure by equipment class, 2026 (millions of units).
Figure 45. Estimated installed base by vendor for routers, switches, firewalls and SD-WAN edges, 2026 (millions of units).
Figure 46. Vendor PQC readiness versus installed-base weight, October 2026.
Figure 47. PQC-capable share of the network infrastructure installed base by equipment class, 2026–2037.
Figure 48. PQC-capable versus classical-only network devices in service, 2026–2037 (millions of units).
Figure 49. Migration and managed services versus core technology and PQC product markets 2027–2037 (millions USD).
Figure 50. Quantum-safe migration and managed services market by category 2027–2037 (millions USD).
Figure 51. Shift in the quantum-safe services mix, 2027 versus 2037 (% of services market).

+357 96 030922
info@marketpublishers.com

Figure 52. The quantum-safe services provider landscape.
Figure 53. Core quantum cybersecurity technology market by end-user group, 2027–2037 (millions USD).
Figure 54. Share of the core quantum cybersecurity technology market by end-user group, 2037.
Figure 55. Growth rate of the core quantum cybersecurity technology market by end user, CAGR 2027–2037 (%).
Figure 56. Quantum-safe migration programme and peak spending windows by sector, 2024–2037.
Figure 57. End-user opportunity matrix: regulatory urgency versus growth potential.
Figure 58. Structure of the quantum cybersecurity industry by participant type.
Figure 59. Selected quantum cybersecurity-related M&A transactions, 2022–October 2026.
Figure 60. Approximate disclosed private funding by quantum cybersecurity segment, 2020–October 2026 (millions USD).
Figure 61. Competitive positioning of selected quantum cybersecurity vendors.
Figure 62. Quantum cybersecurity market drivers and restraints.
Figure 63. Net impact of drivers and restraints by period (weighted impact index).
Figure 64. SWOT analysis of the quantum cybersecurity market.
Figure 65. Technology readiness level of quantum cybersecurity market elements, 2026.
Figure 66. Global quantum cybersecurity market — core technology vs. migration and managed services 2027–2037 (millions USD).
Figure 67. Year-on-year growth of the core and total quantum cybersecurity market 2028–2037 (%).
Figure 68. Core quantum cybersecurity technology market by segment 2027–2037 (millions USD).
Figure 69. Growth trajectories of the five core segments 2027–2037 (millions USD).
Figure 70. Shift in core market segment shares, 2027 vs. 2037 (%).
Figure 71. QKD systems market by type 2027–2037 (millions USD).
Figure 72. Quantum-safe migration and managed services market by category 2027–2037 (millions USD).
Figure 73. Core quantum cybersecurity market by technology approach, 2037 (% of value).
Figure 74. Products TAM by cryptographic approach, 2027–2037 (millions USD).
Figure 75. Migration and managed services TAM by cryptographic approach, 2027–2037 (millions USD).
Figure 76. Total TAM by cryptographic approach, 2027–2037 (millions USD).
Figure 77. Share of total TAM by cryptographic approach, 2027 vs 2037.

+357 96 030922
info@marketpublishers.com

Figure 78. Cumulative TAM by cryptographic approach, 2027–2037 (US$ billion).
Figure 79. Core quantum cybersecurity market by end-user sector, 2037 (millions USD).
Figure 80. Core quantum cybersecurity market by region 2027–2037 (millions USD).
Figure 81. Total quantum cybersecurity market — scenario band 2027–2037 (millions USD).
Figure 82. Core quantum cybersecurity market by region 2027–2037 (millions USD).
Figure 83. Regional share of the core quantum cybersecurity market, 2027.
Figure 84. Regional share of the core quantum cybersecurity market, 2037.
Figure 85. QKD systems market by region 2027–2037 (millions USD).

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: The Quantum Cybersecurity Market 2027-2037

Product link: https://marketpublishers.com/r/Q0992327FBF4EN.html

Price: US$ 1,650.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/Q0992327FBF4EN.html