+357 96 030922
info@marketpublishers.com

Quantum-Safe Cybersecurity Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Solution Type, Security Type, Deployment Mode, Organization Size, End User and By Geography

https://marketpublishers.com/r/Q631A6DB6D85EN.html
Date: June 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: Q631A6DB6D85EN

Abstracts

According to Stratistics MRC, the Global Quantum-Safe Cybersecurity Market is accounted for $5.8 billion in 2026 and is expected to reach $13.8 billion by 2034 growing at a CAGR of 11.4% during the forecast period. Quantum-safe cybersecurity refers to advanced security frameworks and cryptographic technologies designed to protect digital systems and data from potential threats posed by quantum computing. It focuses on implementing post-quantum cryptography, quantum-resistant encryption algorithms, and secure communication protocols capable of withstanding attacks from future quantum computers. As quantum computing advances, traditional encryption methods may become vulnerable, increasing the need for quantum-safe solutions across finance, healthcare, government, defense, and telecommunications sectors. These cybersecurity measures help organizations ensure long-term data protection, regulatory compliance, and resilience against evolving next-generation cyber threats.

Market Dynamics:

Driver:

NIST post-quantum standard finalization

The National Institute of Standards and Technology's finalization of post-quantum cryptographic standards in 2024, including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures, has converted quantum-safe cryptography from academic research to an actionable enterprise security procurement requirement

+357 96 030922
info@marketpublishers.com

backed by government regulatory authority. United States Office of Management and Budget memoranda mandating federal agency migration timelines to quantum-resistant algorithms are creating compliance-driven procurement demand across government contractors, defense suppliers, and regulated financial institutions that must align cryptographic practices with federal cybersecurity standards.

Restraint:

Migration complexity and legacy infrastructure

Replacing classical cryptographic implementations embedded across decades of enterprise software, hardware security modules, network appliances, and operational technology systems with quantum-safe algorithm alternatives requires comprehensive cryptographic inventory assessment, algorithm agility redesign, and coordinated update cycles across complex heterogeneous IT environments that most organizations lack the operational maturity to execute efficiently. Performance overhead of post-quantum algorithms compared to classical alternatives, particularly the larger key sizes and computational requirements of lattice-based schemes on resource-constrained IoT devices and legacy embedded systems, creates technical feasibility barriers for comprehensive enterprise-wide migration within near-term regulatory compliance windows.

Opportunity:

Harvest now decrypt later defense

Growing enterprise awareness of harvest now decrypt later attack strategies in which sophisticated nation-state threat actors are archiving encrypted network traffic and sensitive data today for future decryption using quantum computing systems expected within five to fifteen years is creating immediate urgency for quantum-safe encryption adoption across organizations holding long-lived sensitive data assets in healthcare, defense, financial services, and intellectual property-intensive industries. Intelligence agency warnings from NSA, GCHQ, and ANSSI identifying quantum computing as a near-term strategic threat to classified and commercially sensitive communications are elevating board-level cybersecurity investment mandates for quantum-safe cryptographic migration programs.

Threat:

+357 96 030922
info@marketpublishers.com

Quantum timeline uncertainty investment caution

Significant expert disagreement on practical quantum computing timelines capable of breaking current public key cryptography, ranging from five years to beyond thirty years in published forecasts, creates enterprise budget prioritization uncertainty that delays quantum-safe security investment in organizations competing for limited cybersecurity capital expenditure against immediate threat remediation priorities. Competing vendor narratives around quantum readiness timelines and algorithm selection, combined with the evolving nature of NIST standardization processes and potential future algorithm vulnerabilities in selected post-quantum candidates, create technical uncertainty that conservative enterprise security architects use to defer migration program initiation.

Covid-19 Impact:

Pandemic-accelerated digital transformation expanded the attack surface, requiring quantum-safe protection as organizations rapidly deployed cloud infrastructure, remote access systems, and digital transaction platforms containing sensitive data with long-term confidentiality requirements. Government emergency communication infrastructure deployed during pandemic response highlighted critical dependency on cryptographic security systems requiring quantum-safe upgrading. Post-pandemic, accelerating government regulatory mandates for quantum-safe cryptographic migration across federal systems and critical infrastructure operators are driving enterprise adoption timelines across all major verticals.

The services segment is expected to be the largest during the forecast period

The services segment is expected to account for the largest market share during the forecast period, due to the high complexity of quantum-safe cryptographic migration programs requiring expert consulting, cryptographic inventory assessment, algorithm selection guidance, implementation validation, and ongoing managed security services that most enterprise organizations cannot execute independently without specialized post-quantum security expertise. Professional services engagements designing quantum-safe migration roadmaps, conducting cryptographic agility assessments, and implementing hybrid classical and post-quantum cryptographic architectures command premium consulting fees from government agencies, financial institutions, and defense contractors facing regulatory compliance timelines.

The lattice-based cryptography segment is expected to have the highest CAGR during the forecast period

+357 96 030922
info@marketpublishers.com

Over the forecast period, the lattice-based cryptography segment is predicted to witness the highest growth rate, driven by the selection of lattice-based algorithms CRYSTALS-Kyber and CRYSTALS-Dilithium as primary NIST post-quantum cryptographic standards for key encapsulation and digital signatures, respectively, establishing lattice-based schemes as the dominant commercial implementation pathway for enterprise quantum-safe cryptographic deployments. The strong mathematical security foundations of lattice problems and favorable performance characteristics of lattice-based algorithms relative to other post-quantum candidates across general-purpose computing environments are driving implementation library development, hardware acceleration integration, and software library adoption across enterprise security platform vendors.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, due to the United States federal government quantum-safe cryptography migration mandates creating the world's largest institutional procurement program for post-quantum security solutions across defense agencies, civilian departments, and regulated financial institutions operating under federal compliance frameworks. The concentration of quantum computing research programs and quantum-safe security technology vendors, including IBM Corporation, Microsoft Corporation, and PQShield in North America, creates a mature commercial supply ecosystem supporting rapid enterprise adoption.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, due to accelerating national quantum computing investment programs in China, Japan, South Korea, India, and Australia, creating parallel quantum-safe cybersecurity adoption urgency as governments recognize both the offensive quantum computing capabilities of strategic competitors and the defensive necessity of post-quantum cryptographic migration across critical national infrastructure. China's substantial quantum computing research investment and simultaneous domestic post-quantum cryptography standardization program through the OSCCA are driving parallel quantum-safe security procurement across Chinese financial institutions, telecommunications operators, and government agencies.

Key players in the market

+357 96 030922
info@marketpublishers.com

Some of the key players in Quantum-Safe Cybersecurity Market include IBM Corporation, Intel Corporation, Microsoft Corporation, Google LLC (Alphabet Inc.), Amazon Web Services Inc., Thales Group, ID Quantique, Toshiba Corporation, Quantum Xchange, PQShield, SandboxAQ, ISARA Corporation, Crypto4A Technologies Inc., QuintessenceLabs Pty Ltd, MagiQ Technologies Inc., Nokia Corporation, Fortinet Inc., and Palo Alto Networks Inc.

Key Developments:

In April 2026, SandboxAQ secured a contract with a major US federal agency to conduct an enterprise-wide cryptographic inventory assessment and develop a post-quantum migration roadmap covering classified and unclassified network infrastructure.

In March 2026, PQShield announced a partnership with a leading semiconductor manufacturer to integrate post-quantum cryptographic IP cores into next-generation secure microcontroller and SoC designs for IoT and automotive applications.

In February 2026, Thales Group released a quantum-safe hardware security module firmware update enabling NIST-standardized post-quantum algorithm support across its Luna and payShield HSM product families for banking and government deployments.

Components Covered:

- Solutions
- Services

Solution Types Covered:

- Lattice-Based Cryptography
- Hash-Based Cryptography
- Code-Based Cryptography
- Multivariate Cryptography

+357 96 030922
info@marketpublishers.com

Hybrid Cryptographic Solutions

Security Types Covered:

Network Security

Application Security

Data Security

Identity & Access Security

Cloud Security

Deployment Modes Covered:

On-Premises

Cloud-Based

Hybrid

Organization Sizes Covered:

Large Enterprises

Small & Medium Enterprises (SMEs)

End Users Covered:

Banking, Financial Services & Insurance (BFSI)

Government & Defense

Healthcare & Life Sciences

+357 96 030922
info@marketpublishers.com

- IT & Telecommunications
- Energy & Utilities
- Retail & E-Commerce
- Manufacturing

Regions Covered:

- North America
  - United States
  - Canada
  - Mexico
- Europe
  - United Kingdom
  - Germany
  - France
  - Italy
  - Spain
  - Netherlands
  - Belgium
  - Sweden
  - Switzerland

+357 96 030922
info@marketpublishers.com

- Poland
- Rest of Europe

Asia Pacific

- China
- Japan
- India
- South Korea
- Australia
- Indonesia
- Thailand
- Malaysia
- Singapore
- Vietnam
- Rest of Asia Pacific

South America

- Brazil
- Argentina
- Colombia
- Chile

+357 96 030922
info@marketpublishers.com

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of Africa

What our report offers:
- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends

+357 96 030922
info@marketpublishers.com

- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

11 GLOBAL QUANTUM-SAFE CYBERSECURITY MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Quantum-Safe Cybersecurity Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Solution Type, Security Type, Deployment Mode, Organization Size, End User and By Geography

Product link: https://marketpublishers.com/r/Q631A6DB6D85EN.html

Price: US$ 4,150.00 (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/Q631A6DB6D85EN.html