

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 Statistics 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

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:

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

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

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

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

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

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

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

- 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

Contents

1 EXECUTIVE SUMMARY

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

2 RESEARCH FRAMEWORK

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
 - 2.4.1 Data Collection (Primary and Secondary)
 - 2.4.2 Data Modeling and Estimation Techniques
 - 2.4.3 Data Validation and Triangulation
 - 2.4.4 Analytical and Forecasting Approach

3 MARKET DYNAMICS AND TREND ANALYSIS

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

4 COMPETITIVE AND STRATEGIC ASSESSMENT

- 4.1 Porter's Five Forces Analysis
 - 4.1.1 Supplier Bargaining Power
 - 4.1.2 Buyer Bargaining Power
 - 4.1.3 Threat of Substitutes
 - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

5 GLOBAL QUANTUM-SAFE CYBERSECURITY MARKET, BY COMPONENT

- 5.1 Solutions
- 5.2 Services

6 GLOBAL QUANTUM-SAFE CYBERSECURITY MARKET, BY SOLUTION TYPE

- 6.1 Lattice-Based Cryptography
- 6.2 Hash-Based Cryptography
- 6.3 Code-Based Cryptography
- 6.4 Multivariate Cryptography
- 6.5 Hybrid Cryptographic Solutions

7 GLOBAL QUANTUM-SAFE CYBERSECURITY MARKET, BY SECURITY TYPE

- 7.1 Network Security
- 7.2 Application Security
- 7.3 Data Security
- 7.4 Identity & Access Security
- 7.5 Cloud Security

8 GLOBAL QUANTUM-SAFE CYBERSECURITY MARKET, BY DEPLOYMENT MODE

- 8.1 On-Premises
- 8.2 Cloud-Based
- 8.3 Hybrid

9 GLOBAL QUANTUM-SAFE CYBERSECURITY MARKET, BY ORGANIZATION SIZE

- 9.1 Large Enterprises
- 9.2 Small & Medium Enterprises (SMEs)

10 GLOBAL QUANTUM-SAFE CYBERSECURITY MARKET, BY END USER

- 10.1 Banking, Financial Services & Insurance (BFSI)
- 10.2 Government & Defense
- 10.3 Healthcare & Life Sciences
- 10.4 IT & Telecommunications
- 10.5 Energy & Utilities
- 10.6 Retail & E-Commerce
- 10.7 Manufacturing

11 GLOBAL QUANTUM-SAFE CYBERSECURITY MARKET, BY GEOGRAPHY

- 11.1 North America
 - 11.1.1 United States
 - 11.1.2 Canada
 - 11.1.3 Mexico
- 11.2 Europe
 - 11.2.1 United Kingdom
 - 11.2.2 Germany
 - 11.2.3 France
 - 11.2.4 Italy
 - 11.2.5 Spain
 - 11.2.6 Netherlands
 - 11.2.7 Belgium
 - 11.2.8 Sweden
 - 11.2.9 Switzerland
 - 11.2.10 Poland
 - 11.2.11 Rest of Europe
- 11.3 Asia Pacific
 - 11.3.1 China
 - 11.3.2 Japan
 - 11.3.3 India
 - 11.3.4 South Korea
 - 11.3.5 Australia
 - 11.3.6 Indonesia
 - 11.3.7 Thailand
 - 11.3.8 Malaysia
 - 11.3.9 Singapore
 - 11.3.10 Vietnam
 - 11.3.11 Rest of Asia Pacific

11.4 South America

11.4.1 Brazil

11.4.2 Argentina

11.4.3 Colombia

11.4.4 Chile

11.4.5 Peru

11.4.6 Rest of South America

11.5 Rest of the World (RoW)

11.5.1 Middle East

11.5.1.1 Saudi Arabia

11.5.1.2 United Arab Emirates

11.5.1.3 Qatar

11.5.1.4 Israel

11.5.1.5 Rest of Middle East

11.5.2 Africa

11.5.2.1 South Africa

11.5.2.2 Egypt

11.5.2.3 Morocco

11.5.2.4 Rest of Africa

12 STRATEGIC MARKET INTELLIGENCE

12.1 Industry Value Network and Supply Chain Assessment

12.2 White-Space and Opportunity Mapping

12.3 Product Evolution and Market Life Cycle Analysis

12.4 Channel, Distributor, and Go-to-Market Assessment

13 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

13.1 Mergers and Acquisitions

13.2 Partnerships, Alliances, and Joint Ventures

13.3 New Product Launches and Certifications

13.4 Capacity Expansion and Investments

13.5 Other Strategic Initiatives

14 COMPANY PROFILES

14.1 IBM Corporation

14.2 Intel Corporation

- 14.3 Microsoft Corporation
- 14.4 Google LLC (Alphabet Inc.)
- 14.5 Amazon Web Services Inc.
- 14.6 Thales Group
- 14.7 ID Quantique
- 14.8 Toshiba Corporation
- 14.9 Quantum Xchange
- 14.10 PQShield
- 14.11 SandboxAQ
- 14.12 ISARA Corporation
- 14.13 Crypto4A Technologies Inc.
- 14.14 QuintessenceLabs Pty Ltd
- 14.15 MagiQ Technologies Inc.
- 14.16 Nokia Corporation
- 14.17 Fortinet Inc.
- 14.18 Palo Alto Networks Inc.

List Of Tables

LIST OF TABLES

Table 1 Global Quantum-Safe Cybersecurity Market Outlook, By Region (2023-2034) (\$MN)

Table 2 Global Quantum-Safe Cybersecurity Market Outlook, By Component (2023-2034) (\$MN)

Table 3 Global Quantum-Safe Cybersecurity Market Outlook, By Solutions (2023-2034) (\$MN)

Table 4 Global Quantum-Safe Cybersecurity Market Outlook, By Services (2023-2034) (\$MN)

Table 5 Global Quantum-Safe Cybersecurity Market Outlook, By Solution Type (2023-2034) (\$MN)

Table 6 Global Quantum-Safe Cybersecurity Market Outlook, By Lattice-Based Cryptography (2023-2034) (\$MN)

Table 7 Global Quantum-Safe Cybersecurity Market Outlook, By Hash-Based Cryptography (2023-2034) (\$MN)

Table 8 Global Quantum-Safe Cybersecurity Market Outlook, By Code-Based Cryptography (2023-2034) (\$MN)

Table 9 Global Quantum-Safe Cybersecurity Market Outlook, By Multivariate Cryptography (2023-2034) (\$MN)

Table 10 Global Quantum-Safe Cybersecurity Market Outlook, By Hybrid Cryptographic Solutions (2023-2034) (\$MN)

Table 11 Global Quantum-Safe Cybersecurity Market Outlook, By Security Type (2023-2034) (\$MN)

Table 12 Global Quantum-Safe Cybersecurity Market Outlook, By Network Security (2023-2034) (\$MN)

Table 13 Global Quantum-Safe Cybersecurity Market Outlook, By Application Security (2023-2034) (\$MN)

Table 14 Global Quantum-Safe Cybersecurity Market Outlook, By Data Security (2023-2034) (\$MN)

Table 15 Global Quantum-Safe Cybersecurity Market Outlook, By Identity & Access Security (2023-2034) (\$MN)

Table 16 Global Quantum-Safe Cybersecurity Market Outlook, By Cloud Security (2023-2034) (\$MN)

Table 17 Global Quantum-Safe Cybersecurity Market Outlook, By Deployment Mode (2023-2034) (\$MN)

Table 18 Global Quantum-Safe Cybersecurity Market Outlook, By On-Premises

(2023-2034) (\$MN)

Table 19 Global Quantum-Safe Cybersecurity Market Outlook, By Cloud-Based

(2023-2034) (\$MN)

Table 20 Global Quantum-Safe Cybersecurity Market Outlook, By Hybrid (2023-2034)

(\$MN)

Table 21 Global Quantum-Safe Cybersecurity Market Outlook, By Organization Size

(2023-2034) (\$MN)

Table 22 Global Quantum-Safe Cybersecurity Market Outlook, By Large Enterprises

(2023-2034) (\$MN)

Table 23 Global Quantum-Safe Cybersecurity Market Outlook, By Small & Medium Enterprises (SMEs) (2023-2034) (\$MN)

Table 24 Global Quantum-Safe Cybersecurity Market Outlook, By End User

(2023-2034) (\$MN)

Table 25 Global Quantum-Safe Cybersecurity Market Outlook, By Banking, Financial Services & Insurance (BFSI) (2023-2034) (\$MN)

Table 26 Global Quantum-Safe Cybersecurity Market Outlook, By Government & Defense (2023-2034) (\$MN)

Table 27 Global Quantum-Safe Cybersecurity Market Outlook, By Healthcare & Life Sciences (2023-2034) (\$MN)

Table 28 Global Quantum-Safe Cybersecurity Market Outlook, By IT & Telecommunications (2023-2034) (\$MN)

Table 29 Global Quantum-Safe Cybersecurity Market Outlook, By Energy & Utilities (2023-2034) (\$MN)

Table 30 Global Quantum-Safe Cybersecurity Market Outlook, By Retail & E-Commerce (2023-2034) (\$MN)

Table 31 Global Quantum-Safe Cybersecurity Market Outlook, By Manufacturing (2023-2034) (\$MN)

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.

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>