+357 96 030922
info@marketpublishers.com

# Post-Quantum Data Security Solutions Market Forecasts to 2034 – Global Analysis By Security Solution (Post-Quantum Encryption, Quantum-Resistant Key Management, Cryptographic Agility Platforms, Quantum-Safe Digital Signatures, and Secure Certificate Management), Cryptographic Approach, Security Layer, Migration Function, Organization Size, End User and By Geography

https://marketpublishers.com/r/PB7D5EF7396AEN.html
Date: August 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: PB7D5EF7396AEN

## Abstracts

According to Stratistics MRC, the Global Post-Quantum Data Security Solutions Market is accounted for $1.5 billion in 2026 and is expected to reach $7.7 billion by 2034 growing at a CAGR of 22.6% during the forecast period. Post-quantum data security solutions refer to cryptographic technologies and platforms designed to protect sensitive information against attacks from quantum computers that can compromise traditional encryption algorithms. These solutions encompass lattice-based, hash-based, and code-based encryption schemes alongside quantum-resistant key management, digital signature, and certificate migration systems. The technology enables organizations to transition existing cryptographic infrastructure to algorithms standardized by NIST that remain secure against both classical and quantum computational threats.

Market Dynamics:

Driver:

Quantum Computing Threat Awareness

+357 96 030922
info@marketpublishers.com

The accelerating development of quantum computing capabilities is driving urgent enterprise and government investment in cryptographic migration strategies. Organizations are increasingly aware that current public-key encryption systems will become vulnerable to quantum attacks within the forecast decade. Regulatory bodies and standards organizations are mandating transition timelines that compel proactive procurement of quantum-resistant solutions. This threat awareness is creating substantial commercial demand across banking, defense, healthcare, and critical infrastructure sectors.

Restraint:

Migration Complexity Burden

The extensive engineering effort required to inventory, replace, and validate cryptographic algorithms across complex enterprise IT ecosystems presents a formidable barrier to rapid adoption. Organizations operate thousands of interconnected systems and applications that each require individual cryptographic assessment and upgrade. The risk of introducing compatibility issues during algorithm replacement creates legitimate operational concerns that delay migration initiatives. These complexity factors extend implementation timelines from months to multiple years for large enterprises.

Opportunity:

Cryptographic Agility Platforms

The development of cryptographic agility platforms enabling rapid algorithm substitution without extensive system re-engineering represents a significant market opportunity. These solutions provide centralized discovery, inventory, and automated replacement capabilities that substantially reduce migration costs and timelines. The emergence of hybrid cryptographic approaches combining classical and post-quantum algorithms during transition periods further lowers adoption barriers. Vendors offering comprehensive agility platforms are positioned to capture substantial share of the enterprise migration market.

Threat:

Standards Uncertainty Risks

+357 96 030922
info@marketpublishers.com

Ongoing evolution of post-quantum cryptography standards and potential discovery of vulnerabilities in newly standardized algorithms pose significant risks to early adopters. The cryptographic community continues to analyze NIST-selected algorithms, and future breakthroughs could invalidate current investment in specific post-quantum schemes. Organizations may adopt a wait-and-see approach until standards mature, slowing near-term market growth. High-profile algorithm failures could undermine enterprise confidence in the entire post-quantum transition.

Covid-19 Impact:

The pandemic initially disrupted cybersecurity consulting services and delayed post-quantum cryptography assessment projects across government and enterprise clients. During the mid-pandemic period, accelerated digital transformation and remote work expansion dramatically increased the attack surface for organizations, highlighting long-term cryptographic vulnerabilities. Post-pandemic, the market has experienced explosive growth as governments finalized NIST standardization and mandated transition timelines, with supply chain security concerns further driving investment in quantum-resistant infrastructure.

The post-quantum encryption segment is expected to be the largest during the forecast period

The post-quantum encryption segment is expected to account for the largest market share during the forecast period, due to its foundational role in protecting data confidentiality across all digital communication and storage systems. This segment encompasses lattice-based and code-based encryption schemes that replace vulnerable RSA and elliptic curve implementations. Government and defense organizations are prioritizing encryption migration as the highest-impact component of their quantum-resistant strategies. The critical nature of data protection ensures that encryption solutions receive the largest portion of security budgets.

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

Over the forecast period, the hash-based cryptography segment is predicted to witness the highest growth rate, driven by its strong security guarantees based on well-understood hash function properties and relatively straightforward implementation requirements. This approach is gaining traction for digital signature applications where long-term document integrity is essential. The maturity of hash-based theoretical

+357 96 030922
info@marketpublishers.com

foundations and reduced implementation complexity compared to lattice-based alternatives are accelerating enterprise adoption. Organizations seeking conservative, proven quantum-resistant approaches are increasingly favoring hash-based solutions.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, due to early government mandates for post-quantum cryptographic migration and the concentration of leading cybersecurity vendors in the United States. The region benefits from NIST standardization leadership and substantial Department of Defense investment in quantum-resistant infrastructure. Major players including IBM Corporation, Microsoft Corporation, and Cloudflare, Inc. are headquartered in this region and actively developing post-quantum security platforms. The mature regulatory environment continues to drive compliance-oriented spending.

Region with highest CAGR:

Over the forecast period, the Europe region is anticipated to exhibit the highest CAGR, due to aggressive regulatory requirements for quantum-resistant cryptography and substantial government funding for cybersecurity research across the European Union. Countries including Germany, France, and the United Kingdom are implementing national quantum strategies that mandate cryptographic transition timelines for critical infrastructure. The region's strong tradition in cryptographic research and presence of specialized vendors create favorable conditions for market expansion. These policy dynamics position Europe as the fastest-growing regional market.

Key players in the market

Some of the key players in Post-Quantum Data Security Solutions Market include IBM Corporation, Microsoft Corporation, Google LLC, Amazon Web Services, Inc., Thales S.A., Cloudflare, Inc., Cisco Systems, Inc., Broadcom Inc., Entrust Corporation, Quantinuum Ltd., Post-Quantum Solutions Ltd., SandboxAQ LLC, ISARA Corporation, SEALSQ Corp., QuSecure, Inc., InfoSec Global Inc. and Keyfactor, Inc..

Key Developments:

In August 2026, IBM Corporation launched a comprehensive post-quantum cryptography migration platform with automated cryptographic discovery and algorithm inventory for enterprise transition to NIST-standardized schemes.

+357 96 030922
info@marketpublishers.com

In July 2026, Microsoft Corporation introduced quantum-resistant TLS implementations across Azure services, enabling customers to protect data in transit against future quantum computing threats without application changes.

In June 2026, Thales S.A. released a hardware security module with native post-quantum algorithm support, providing quantum-resistant key generation and digital signature capabilities for government and defense clients.

Security Solutions Covered:

- Post-Quantum Encryption
- Quantum-Resistant Key Management
- Cryptographic Agility Platforms
- Quantum-Safe Digital Signatures
- Secure Certificate Management

Cryptographic Approaches Covered:

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

Security Layers Covered:

- Application Security

+357 96 030922
info@marketpublishers.com

Network Security

Database Security

Cloud Security

Endpoint Security

Migration Functions Covered:

Cryptographic Discovery

Vulnerability Assessment

Algorithm Inventory

Certificate Migration

Key Replacement

Organization Sizes Covered:

Large Enterprises

Medium-Sized Enterprises

Small Enterprises

Government Agencies

Defense Organizations

End Users Covered:

Banking and Financial Services

+357 96 030922
info@marketpublishers.com

- Government and Defense
- Healthcare and Life Sciences
- Information Technology
- Telecommunications

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
- Peru

+357 96 030922
info@marketpublishers.com

- 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)

+357 96 030922
info@marketpublishers.com

- 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

+357 96 030922
info@marketpublishers.com

# 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

+357 96 030922
info@marketpublishers.com

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

**5 GLOBAL POST-QUANTUM DATA SECURITY SOLUTIONS MARKET, BY SECURITY SOLUTION**

5.1 Post-Quantum Encryption
5.2 Quantum-Resistant Key Management
5.3 Cryptographic Agility Platforms
5.4 Quantum-Safe Digital Signatures
5.5 Secure Certificate Management

**6 GLOBAL POST-QUANTUM DATA SECURITY SOLUTIONS MARKET, BY CRYPTOGRAPHIC APPROACH**

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

**7 GLOBAL POST-QUANTUM DATA SECURITY SOLUTIONS MARKET, BY SECURITY LAYER**

7.1 Application Security
7.2 Network Security
7.3 Database Security
7.4 Cloud Security
7.5 Endpoint Security

**8 GLOBAL POST-QUANTUM DATA SECURITY SOLUTIONS MARKET, BY MIGRATION FUNCTION**

8.1 Cryptographic Discovery
8.2 Vulnerability Assessment
8.3 Algorithm Inventory
8.4 Certificate Migration
8.5 Key Replacement

+357 96 030922
info@marketpublishers.com

## 9 GLOBAL POST-QUANTUM DATA SECURITY SOLUTIONS MARKET, BY ORGANIZATION SIZE

9.1 Large Enterprises
9.2 Medium-Sized Enterprises
9.3 Small Enterprises
9.4 Government Agencies
9.5 Defense Organizations

## 10 GLOBAL POST-QUANTUM DATA SECURITY SOLUTIONS MARKET, BY END USER

10.1 Banking and Financial Services
10.2 Government and Defense
10.3 Healthcare and Life Sciences
10.4 Information Technology
10.5 Telecommunications

## 11 GLOBAL POST-QUANTUM DATA SECURITY SOLUTIONS 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

+357 96 030922
info@marketpublishers.com

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**

+357 96 030922
info@marketpublishers.com

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 Microsoft Corporation
14.3 Google LLC
14.4 Amazon Web Services, Inc.
14.5 Thales S.A.
14.6 Cloudflare, Inc.
14.7 Cisco Systems, Inc.
14.8 Broadcom Inc.
14.9 Entrust Corporation
14.10 Quantinuum Ltd.
14.11 Post-Quantum Solutions Ltd.
14.12 SandboxAQ LLC
14.13 ISARA Corporation
14.14 SEALSQ Corp.
14.15 QuSecure, Inc.
14.16 InfoSec Global Inc.
14.17 Keyfactor, Inc.

+357 96 030922
info@marketpublishers.com

# List Of Tables

## LIST OF TABLES

Table 1 Global Post-Quantum Data Security Solutions Market Outlook, By Region (2023-2034) ($MN)
Table 2 Global Post-Quantum Data Security Solutions Market Outlook, By Security Solution (2023-2034) ($MN)
Table 3 Global Post-Quantum Data Security Solutions Market Outlook, By Post-Quantum Encryption (2023-2034) ($MN)
Table 4 Global Post-Quantum Data Security Solutions Market Outlook, By Quantum-Resistant Key Management (2023-2034) ($MN)
Table 5 Global Post-Quantum Data Security Solutions Market Outlook, By Cryptographic Agility Platforms (2023-2034) ($MN)
Table 6 Global Post-Quantum Data Security Solutions Market Outlook, By Quantum-Safe Digital Signatures (2023-2034) ($MN)
Table 7 Global Post-Quantum Data Security Solutions Market Outlook, By Secure Certificate Management (2023-2034) ($MN)
Table 8 Global Post-Quantum Data Security Solutions Market Outlook, By Cryptographic Approach (2023-2034) ($MN)
Table 9 Global Post-Quantum Data Security Solutions Market Outlook, By Lattice-Based Cryptography (2023-2034) ($MN)
Table 10 Global Post-Quantum Data Security Solutions Market Outlook, By Hash-Based Cryptography (2023-2034) ($MN)
Table 11 Global Post-Quantum Data Security Solutions Market Outlook, By Code-Based Cryptography (2023-2034) ($MN)
Table 12 Global Post-Quantum Data Security Solutions Market Outlook, By Multivariate Cryptography (2023-2034) ($MN)
Table 13 Global Post-Quantum Data Security Solutions Market Outlook, By Hybrid Cryptography (2023-2034) ($MN)
Table 14 Global Post-Quantum Data Security Solutions Market Outlook, By Security Layer (2023-2034) ($MN)
Table 15 Global Post-Quantum Data Security Solutions Market Outlook, By Application Security (2023-2034) ($MN)
Table 16 Global Post-Quantum Data Security Solutions Market Outlook, By Network Security (2023-2034) ($MN)
Table 17 Global Post-Quantum Data Security Solutions Market Outlook, By Database Security (2023-2034) ($MN)
Table 18 Global Post-Quantum Data Security Solutions Market Outlook, By Cloud

+357 96 030922
info@marketpublishers.com

Security (2023-2034) ($MN)
Table 19 Global Post-Quantum Data Security Solutions Market Outlook, By Endpoint Security (2023-2034) ($MN)
Table 20 Global Post-Quantum Data Security Solutions Market Outlook, By Migration Function (2023-2034) ($MN)
Table 21 Global Post-Quantum Data Security Solutions Market Outlook, By Cryptographic Discovery (2023-2034) ($MN)
Table 22 Global Post-Quantum Data Security Solutions Market Outlook, By Vulnerability Assessment (2023-2034) ($MN)
Table 23 Global Post-Quantum Data Security Solutions Market Outlook, By Algorithm Inventory (2023-2034) ($MN)
Table 24 Global Post-Quantum Data Security Solutions Market Outlook, By Certificate Migration (2023-2034) ($MN)
Table 25 Global Post-Quantum Data Security Solutions Market Outlook, By Key Replacement (2023-2034) ($MN)
Table 26 Global Post-Quantum Data Security Solutions Market Outlook, By Organization Size (2023-2034) ($MN)
Table 27 Global Post-Quantum Data Security Solutions Market Outlook, By Large Enterprises (2023-2034) ($MN)
Table 28 Global Post-Quantum Data Security Solutions Market Outlook, By Medium-Sized Enterprises (2023-2034) ($MN)
Table 29 Global Post-Quantum Data Security Solutions Market Outlook, By Small Enterprises (2023-2034) ($MN)
Table 30 Global Post-Quantum Data Security Solutions Market Outlook, By Government Agencies (2023-2034) ($MN)
Table 31 Global Post-Quantum Data Security Solutions Market Outlook, By Defense Organizations (2023-2034) ($MN)
Table 32 Global Post-Quantum Data Security Solutions Market Outlook, By End User (2023-2034) ($MN)
Table 33 Global Post-Quantum Data Security Solutions Market Outlook, By Banking and Financial Services (2023-2034) ($MN)
Table 34 Global Post-Quantum Data Security Solutions Market Outlook, By Government and Defense (2023-2034) ($MN)
Table 35 Global Post-Quantum Data Security Solutions Market Outlook, By Healthcare and Life Sciences (2023-2034) ($MN)
Table 36 Global Post-Quantum Data Security Solutions Market Outlook, By Information Technology (2023-2034) ($MN)
Table 37 Global Post-Quantum Data Security Solutions Market Outlook, By Telecommunications (2023-2034) ($MN)

+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: Post-Quantum Data Security Solutions Market Forecasts to 2034 – Global Analysis By Security Solution (Post-Quantum Encryption, Quantum-Resistant Key Management, Cryptographic Agility Platforms, Quantum-Safe Digital Signatures, and Secure Certificate Management), Cryptographic Approach, Security Layer, Migration Function, Organization Size, End User and By Geography

Product link: https://marketpublishers.com/r/PB7D5EF7396AEN.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/PB7D5EF7396AEN.html