+357 96 030922
info@marketpublishers.com

Post-Quantum Cryptography (PQC) Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Solution (Quantum-Safe Hardware, Quantum-Resistant Algorithms, Quantum-Safe Cryptographic Libraries, Quantum-Safe VPN, Email Service, and Messaging Systems, Quantum-Safe Blockchain Solutions, Quantum-Safe Authentication Solutions, Quantum-Resistant Encryption Solutions), By Organization Size (Large Enterprises, SMEs), By Vertical (BFSI, Government & Defense, Healthcare, IT & ITES, Retail & E-Commerce, Others), By Region, By Competition 2020-2030F

https://marketpublishers.com/r/P53710D88C3AEN.html
Date: August 2025
Pages: 185
Price: US$ 4,500.00 (Single User License)
ID: P53710D88C3AEN

Abstracts

Market Overview

Global Post-Quantum Cryptography (PQC) Market was valued at USD 297.82 Million in 2024 and is expected to reach USD 2493.97 Million by 2030 with a CAGR of 42.50% through 2030. Post-Quantum Cryptography (PQC) refers to cryptographic algorithms specifically designed to withstand the potential threats posed by quantum computers.

Unlike traditional encryption methods such as RSA and ECC, which are vulnerable to powerful quantum attacks, PQC algorithms are built to offer long-term security in a quantum-enabled world. These algorithms aim to protect data confidentiality, integrity, and authentication, even against the computing power of quantum machines. With

+357 96 030922
info@marketpublishers.com

growing awareness of the risks posed by quantum computing, industries, governments, and security organizations are turning their focus toward PQC as a proactive step to safeguard sensitive information before quantum computers become mainstream.

The Global Post-Quantum Cryptography (PQC) Market is expected to witness significant growth due to increasing awareness of quantum computing threats and the proactive stance of regulatory authorities. Initiatives like the National Institute of Standards and Technology (NIST) PQC standardization project have accelerated global efforts to develop quantum-resistant cryptographic standards. Key industries such as finance, defense, healthcare, and telecommunications recognize the need to secure data that must remain protected for decades. This growing demand is leading to increased investments in PQC research and development, partnerships between academia and cybersecurity firms, and the early integration of PQC solutions into existing digital infrastructures.

The rapid digitalization of critical sectors, combined with ongoing advancements in quantum computing by leading technology companies, is a major factor driving the Global Post-Quantum Cryptography (PQC) Market. Organizations are seeking ways to future-proof their security systems through hybrid cryptography approaches and quantum-safe upgrades. Additionally, the rise of cryptography-as-a-service platforms, stricter data protection regulations, and increasing emphasis on cybersecurity resilience further support the market's growth. As innovations continue and governments prioritize post-quantum security readiness, the Global Post-Quantum Cryptography (PQC) Market is poised to expand, evolving from a specialized research area into an essential element of global cybersecurity strategies.

Key Market Drivers

Rising Quantum Computing Advancements Posing Security Threats

Quantum computing is progressing rapidly, with several technological giants such as IBM, Google, and China’s Quantum Research Group achieving critical milestones in recent years. These advancements have amplified the urgency among enterprises and governments to evaluate their existing cryptographic protocols, which are at risk of becoming obsolete. Quantum algorithms like Shor's Algorithm can potentially break RSA and ECC encryption, making most of today's secure communications vulnerable once quantum computing reaches maturity. The fear of a "harvest now, decrypt later" attack — where encrypted data is stolen today to be decrypted in the future with

+357 96 030922
info@marketpublishers.com

quantum machines — is pushing organizations to invest early in quantum-resistant cryptography.

The Global Post-Quantum Cryptography (PQC) Market is positioned to capitalize on this threat landscape as businesses seek robust protection against the looming quantum threat. With quantum computing no longer a theoretical concept but a developing reality, organizations are prioritizing long-term data security strategies that include PQC solutions. As these developments accelerate, the adoption of PQC becomes not just a security upgrade but a strategic business imperative to protect intellectual property, sensitive transactions, and customer data against potential quantum breaches in the near future. In 2023, IBM introduced its “Condor” quantum processor, featuring 1,121 qubits, marking a substantial leap in quantum hardware development. This achievement demonstrates how quickly quantum computing is advancing toward practical applications. Such milestones intensify the urgency for adopting quantum-resistant cryptographic solutions, directly influencing the growth of the Global Post-Quantum Cryptography (PQC) Market.

Key Market Challenges

Implementation Complexity and Integration with Existing Infrastructure

One of the foremost challenges facing the Global Post-Quantum Cryptography (PQC) Market is the significant complexity associated with implementing quantum-resistant algorithms within existing digital ecosystems. Most enterprises today rely on traditional public key infrastructures (PKI), security protocols, and cryptographic standards that have been deeply embedded across their networks, applications, and devices. These infrastructures were designed around classical cryptographic schemes like RSA and ECC, which are deeply integrated into secure communication protocols such as TLS, VPNs, digital signatures, and authentication systems. Introducing post-quantum algorithms often requires a complete overhaul or substantial modification of these systems, posing logistical, technical, and financial hurdles.

Organizations must address issues like key size increases, performance degradation, and interoperability between classical and post-quantum cryptographic systems. For example, many PQC algorithms have larger key sizes or slower processing speeds compared to traditional algorithms, impacting system performance and bandwidth usage. Additionally, backward compatibility with legacy systems becomes a critical issue, as not all platforms are designed to accommodate new cryptographic primitives. Enterprises must undertake thorough assessments, pilot testing, and often custom

+357 96 030922
info@marketpublishers.com

integration projects to ensure seamless operation—an endeavor that demands skilled personnel, time, and significant investment. This complexity is particularly burdensome for industries operating large-scale legacy systems, such as banking, healthcare, and government sectors, thereby acting as a strong inhibitor to rapid PQC adoption in the Global Post-Quantum Cryptography (PQC) Market.

Key Market Trends

Hybrid Cryptography Deployment Models

A growing trend within the Global Post-Quantum Cryptography (PQC) Market is the increasing adoption of hybrid cryptography models, where post-quantum algorithms are combined with classical encryption methods. This dual approach allows organizations to secure their data transmissions against both current and future threats without fully replacing existing systems. By leveraging hybrid models, enterprises can integrate PQC gradually, reducing the risk of performance loss or interoperability issues while maintaining compliance with current security protocols. This trend is particularly appealing to industries like finance and defense, where the cost of a total system overhaul would be prohibitive and operational risks are high.

The hybrid cryptography trend is also driven by the uncertainty surrounding which PQC algorithms will ultimately become the global standard. By adopting a hybrid strategy, organizations can safeguard sensitive communications today while positioning themselves for smoother transitions as regulatory guidelines evolve. Moreover, many security vendors are starting to offer hybrid cryptography tools as part of their product portfolios, which accelerates market penetration. This trend underscores a practical, risk-averse approach to quantum-safe security implementation, providing a bridge between legacy systems and future-ready encryption, and is contributing positively to the growth dynamics of the Global Post-Quantum Cryptography (PQC) Market.

Key Market Players

IBM Corporation

Microsoft Corporation

Google LLC

Amazon.com, Inc.

+357 96 030922
info@marketpublishers.com

Intel Corporation

Quantinuum Ltd.

ISARA Corporation

SandboxAQ, Inc.

Report Scope:

In this report, the Global Post-Quantum Cryptography (PQC) Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Post-Quantum Cryptography (PQC) Market, By Solution:

Quantum-Safe Hardware

Quantum-Resistant Algorithms

Quantum-Safe Cryptographic Libraries

Quantum-Safe VPN, Email Service, and Messaging Systems

Quantum-Safe Blockchain Solutions

Quantum-Safe Authentication Solutions

Quantum-Resistant Encryption Solutions

Post-Quantum Cryptography (PQC) Market, By Organization Size:

Large Enterprises

SMEs

Post-Quantum Cryptography (PQC) Market, By Vertical:

+357 96 030922
info@marketpublishers.com

- BFSI
- Government & Defense
- Healthcare
- IT & ITES
- Retail & E-Commerce
- Others

Post-Quantum Cryptography (PQC) Market, By Region:

- North America
  - United States
  - Canada
  - Mexico
- Europe
  - Germany
  - France
  - United Kingdom
  - Italy
  - Spain
- Asia Pacific
  - China

+357 96 030922
info@marketpublishers.com

India

Japan

South Korea

Australia

Middle East & Africa

Saudi Arabia

UAE

South Africa

South America

Brazil

Colombia

Argentina

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Post-Quantum Cryptography (PQC) Market.

Available Customizations:

Global Post-Quantum Cryptography (PQC) Market report with the given market data, Tech Sci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

6. NORTH AMERICA POST-QUANTUM CRYPTOGRAPHY (PQC) MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

7. EUROPE POST-QUANTUM CRYPTOGRAPHY (PQC) MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

8. ASIA PACIFIC POST-QUANTUM CRYPTOGRAPHY (PQC) MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

9. MIDDLE EAST & AFRICA POST-QUANTUM CRYPTOGRAPHY (PQC) MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

10. SOUTH AMERICA POST-QUANTUM CRYPTOGRAPHY (PQC) MARKET OUTLOOK

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Post-Quantum Cryptography (PQC) Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Solution (Quantum-Safe Hardware, Quantum-Resistant Algorithms, Quantum-Safe Cryptographic Libraries, Quantum-Safe VPN, Email Service, and Messaging Systems, Quantum-Safe Blockchain Solutions, Quantum-Safe Authentication Solutions, Quantum-Resistant Encryption Solutions), By Organization Size (Large Enterprises, SMEs), By Vertical (BFSI, Government & Defense, Healthcare, IT & ITES, Retail & E-Commerce, Others), By Region, By Competition 2020-2030F

Product link: https://marketpublishers.com/r/P53710D88C3AEN.html

Price: US$ 4,500.00 (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/P53710D88C3AEN.html