

Quantum-Safe Hardware Security Module Market To Reach \$2.57 Billion By 2029 – Report By TBRC

Quantum-Safe Hardware Security Module Market To Reach \$2.57 Billion By 2029 – Report By TBRC

LONDON, GREATER LONDON, UNITED KINGDOM, October 30, 2025

/EINPresswire.com/ -- "Get 20% Off All Global Market Reports With Code

ONLINE20 – Stay Ahead Of Trade Shifts, Macroeconomic Trends, And Industry Disruptors

The Business
Research Company

The Business Research Company

How Much Is The Quantum-Safe Hardware Security Module Market Worth?

The market size for quantum-safe hardware security modules has seen a speedy expansion in the last few years. The market will escalate from \$1.18 billion in 2024 to \$1.39 billion in 2025, marking a compound annual growth rate (CAGR) of 17.0%. Factors such as the augmenting embracement of cloud-based safety solutions, escalating incidents of online security breaches, burgeoning demand for encryption specifically in the banking and finance sector, growing cognizance of threats posed by quantum computing, and a surge in digital transformation initiatives have contributed to this

“

Expected to grow to \$2.57 billion in 2029 at a compound annual growth rate (CAGR) of 16.7%”

The Business Research Company

growth recorded in the historical period.

The market size for quantum-safe hardware security modules is poised for significant expansion in the coming years, with projections suggesting a growth to \$2.57 billion in 2029, demonstrating a compound annual growth rate (CAGR) of 16.7%. This anticipated growth across the forecast period is supported by the escalating demand for post-quantum cryptography solutions, the increasing adoption of blockchain technology across various sectors, heightened awareness and focus on data sovereignty and adherence to regulatory standards, growing needs for secured multi-cloud environments, and increased investments in next-generation payment mechanisms. Key trends for the forecast period encompass the formulation of standardization frameworks,

the inception of hybrid cryptography solutions, integration with enterprise-wide security platforms, innovations in designs resistant to tampering, and advancements in key management competencies.

Download a free sample of the quantum-safe hardware security module market report:

<https://www.thebusinessresearchcompany.com/sample.aspx?id=28781&type=smp>

What Are The Factors Driving The Quantum-Safe Hardware Security Module Market?

The upsurge in cybersecurity threats is anticipated to drive the expansion of the quantum-safe hardware security module market. Cybersecurity threats represent potential harmful activities or incidents that may breach the privacy, reliability, or accessibility of digital platforms, networks, or information. These threats are on the rise because of amplified digitization and connectivity, which widens the breach scope and increases the exposure of more systems and data to possible cyberattacks. The quantum-safe hardware security module bolsters security against these threats by using quantum-resistant encryption to safeguard sensitive information, authentication procedures, and vital digital transactions. For instance, the Australian Department of Defence reported in November 2023 that there had been over 94,000 cybercrime reports to the Australian Cyber Security Centre between 2022 and 2023, marking a 23% surge from the 2021–22 fiscal year. Thus, the escalating frequency of cybersecurity threats is fuelling the expansion of the quantum-safe hardware security module market.

Who Are The Major Players In The Quantum-Safe Hardware Security Module Market?

Major players in the Quantum-Safe Hardware Security Module Global Market Report 2025 include:

- International Business Machines Corporation
- Thales Group
- Infineon Technologies AG
- Atos SE
- Microchip Technology Inc.
- Entrust Solutions Group
- Rambus Inc.
- PQShield Ltd.
- Yubico AB
- Securosys SA

What Are The Key Trends And Market Opportunities In The Quantum-Safe Hardware Security Module Sector?

Leading organizations in the quantum-safe hardware security module (HSM) market are centering their attention on creating cutting-edge solutions like the post-quantum cryptography (pqc) application package to fortify data security against coming quantum risks. This particular package contains software tools and libraries designed to implement quantum-resistant encryption strategies to defend data from quantum computing intrusions. For instance, in April

2025, Uti-Maco Software GmbH, based out of the US, unveiled Quantum Protect, a PQC application package specifically designed for its u.trust Se-Series HSM, accompanied by a complimentary, completely operational simulator. The HSM components support NIST standardized PQC methodologies such as ML-KEM and ML-DSA, and stateful hash-based hermetic systems like LMS and XMSS. These components collectively establish a quantum-safe groundwork for cryptographic applications. Quantum Protect, which can be activated in-field without any hardware replacements, entails a proprietary state management solution, integrates through PKCS #11 and allows organizations to trial PQC algorithms in real-life settings prior to roll out. This reflects the shift in the market towards feasible quantum-safe security solutions.

Which Segment Accounted For The Largest Quantum-Safe Hardware Security Module Market Share?

The quantum-safe hardware security module market covered in this report is segmented as

- 1) By Component: Hardware, Software, Services
- 2) By Deployment Mode: On-Premises, Cloud
- 3) By Organization Size: Small And Medium Enterprises, Large Enterprises
- 4) By Application: Payment Processing, Authentication, Code And Document Signing, Database Encryption, Public Key Infrastructure Or Key Management, Other Applications
- 5) By End-User: Banking Financial And Insurance, Government And Database, Healthcare, Retail, Information Technology And Telecommunications, Other End-Users

Subsegments:

- 1) By Hardware: Physical Security Appliances, Cryptographic Processors, Secure Storage Units, Network Interface Modules
- 2) By Software: Cryptographic Algorithm Libraries, Key Management Platforms, Authentication And Access Control Solutions, Security Monitoring And Analytics Tools
- 3) By Services: Deployment And Integration Services, Consulting And Advisory Services, Support And Maintenance Services, Training And Education Services

View the full quantum-safe hardware security module market report:

<https://www.thebusinessresearchcompany.com/report/quantum-safe-hardware-security-module-global-market-report>

What Are The Regional Trends In The Quantum-Safe Hardware Security Module Market?

In 2024, the Quantum-Safe Hardware Security Module Global Market Report identified North America as the dominant region. Asia-Pacific, however, is predicted to experience the most rapid expansion during the forecast period. The report encompasses a range of regions including Asia-Pacific, Western Europe, Eastern Europe, North America, South America, and the regions of the Middle East and Africa.

Browse Through More Reports Similar to the Global Quantum-Safe Hardware Security Module Market 2025, By [The Business Research Company](#)

Quantum Security Global Market Report 2025

<https://www.thebusinessresearchcompany.com/report/quantum-security-global-market-report>

Quantum Secure Communication Global Market Report 2025

<https://www.thebusinessresearchcompany.com/report/quantum-secure-communication-global-market-report>

Quantum Chip Global Market Report 2025

<https://www.thebusinessresearchcompany.com/report/quantum-chip-global-market-report>

Speak With Our Expert:

Saumya Sahay

Americas +1 310-496-7795

Asia +44 7882 955267 & +91 8897263534

Europe +44 7882 955267

Email: saumyas@tbrc.info

The Business Research Company - www.thebusinessresearchcompany.com

Follow Us On:

• LinkedIn: <https://in.linkedin.com/company/the-business-research-company>"

Oliver Guirdham

The Business Research Company

+44 7882 955267

info@tbrc.info

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/862520937>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.