

Hardware Security Modules Market by Technology (General Purpose Cryptography, Quantum Cryptography), Type (LAN Based /Network Attached, PCI Based/Embedded Plugins, USB Based, Smart Cards), Deployment Type (Cloud, On-premise) - Global Forecast to 2030

<https://marketpublishers.com/r/HF28ACE291B3EN.html>

Date: February 2025

Pages: 320

Price: US\$ 4,950.00 (Single User License)

ID: HF28ACE291B3EN

Abstracts

The hardware security modules market is expected to grow from USD 1.66 billion in 2025 to USD 3.28 billion by 2030 at a CAGR of 14.5% during the forecast period. The hardware security modules market is witnessing a strong growth trend because of the growing rate of data breaches, cyber attacks, and regulatory compliance requirements across sectors. As business organizations deal with huge volumes of sensitive information, secure encryption key management and cryptography operations have turned into a mission-critical priority. The unprecedented growth of electronic banking, monetary transactions, and identity management technologies is driving need for secure hardware-based security frameworks that provide integrity, authentication, and confidentiality to data.

“Secure Socket Layer (SSL) and Transport Layer Security (TLS) application to grow at high CAGR for the hardware security modules market during the forecast period.”

The hardware security module market for SSL and TLS applications is expected to grow at the highest CAGR during the forecast period till 2030. The growth is driven by the rising demand for secure data transmission, encrypted web communications, and authentication in an growing digital landscape. Companies are prioritizing remote access, and web-based applications, protection of SSL/TLS certificates, private keys, and cryptographic processes as they move to cloud computing. The proliferation of

encrypted communication channels has highlighted the importance of hardware-based security solutions such as HSMs. HSMs provide tamper-proof storage and management of cryptographic keys, which protects against cyber attacks like man-in-the-middle (MITM) attacks, phishing, and SSL/TLS certificate compromise. Further, the increasing adoption of IoT, 5G, and edge computing, in which encrypted communication is essential to protect data exchanges between connected things, networks, and applications, drives the market growth.

“General-purpose Cryptography to account the largest market share in the market during the forecast period.”

The market for general-purpose cryptography is anticipated to have the highest market share as the demand for secure data protection is on the rise across various industries and strong key management solutions are required. With digital transformation speeding up and companies moving more operations to the cloud, there is an increased dependence on encryption to protect sensitive data. General-purpose cryptography covering encryption, decryption, key handling, and the creation of digital signatures is central to protecting exchanges of data in financial institutions, healthcare organizations, government departments, and businesses. Growing adoption of general-purpose cryptography in conjunction with next-generation technologies like blockchain, IoT, and secure payments also drives growth in the segment. Since businesses such as finance and telecommunication are based on secure communication channels and payment transactions, general-purpose cryptographic HSMs are needed to facilitate smooth and secure operations.

“India to witness significant growth in the hardware security modules market during the forecast period.”

Hardware security modules market in India is anticipated to register high CAGR, on account of strong digitalization, growing fintech industry, and rising use of cybersecurity solutions across sectors. India is among the world's fastest-growing economies, and has experienced a boom in online transactions, e-commerce, and cloud computing usage. This has led to a demand for strong encryption solutions such as HSMs to protect sensitive information. The programs of Indian governments, like 'Digital India' and 'Make in India,' are promoting technology uptake in critical industries, including BFSI, healthcare, IT, and manufacturing, further stimulating demand for HSMs. These advancements are enhancing the demand for HSMs. Data protection laws in India are also helping the market grow. India's Digital Personal Data Protection Act (DPDP), 2023, is stressing the necessity of encryption and security measures to protect personal

and financial information. Reserve Bank of India requires stringent cyber security compliance of banks and payments service providers with an incentive of deploying HSMs for authentic key management as well as the encryption of sensitive data. Secondly, the surge in blockchain-driven applications across areas such as logistics, agriculture, and finance also spurred the increase in HSM deployment for authenticating digital signatures and cryptographic securities.

The break-up of the profile of primary participants in the hardware security modules market-

By Company Type: Tier 1 – 20%, Tier 2 – 20%, Tier 3 – 60%

By Designation Type: C Level – 30%, Director Level – 20%, Others – 50%

By Region Type: North America – 20%, Europe – 30%, Asia Pacific – 40%, Rest of the World – 10%

The major players in the hardware security modules market with a significant global presence include Thales (France), IBM (US), Utimaco Management Services GmbH (Germany), Futurex (US), Entrust Corporation (US), and others.

Research Coverage

The report segments the hardware security modules market and forecasts its size by type, technology, deployment type, application, vertical, and region. It also provides a comprehensive review of drivers, restraints, opportunities, and challenges influencing market growth. The report covers qualitative aspects in addition to quantitative aspects of the market.

Reasons to buy the report:

The report will help the market leaders/new entrants in this market with information on the closest approximate revenues for the overall hardware security modules market and related segments. This report will help stakeholders understand the competitive landscape and gain more insights to strengthen their position in the market and plan suitable go-to-market strategies. The report also helps stakeholders understand the pulse of the market and provides them with information on key market drivers, restraints, opportunities, and challenges.

The report provides insights on the following pointers:

Analysis of key drivers (increasing data breaches and cyberattacks, need to comply with stringent data security regulations and standards, growing demand for effective management of cryptographic keys, transition to digital transactions and electronic payments, shift toward SDN and NFV in 5G deployments), restraints (high ownership costs associated with hardware security modules, susceptibility to cyberattacks and security breaches), opportunities (rising volume of data generated by websites and mobile apps, proliferation of connected devices and IoT technologies in smart cities, rise of telemedicine and remote healthcare services, increasing adoption of blockchain and cryptocurrencies, advancements in quantum computing), and challenges (discovering and protecting sensitive data, complexities associated with HSM integration process, rise of complex IT environments)

Product Development/Innovation: Detailed insights on upcoming technologies, research & development activities, and new solution and service launches in the hardware security modules market.

Market Development: Comprehensive information about lucrative markets – the report analyses the hardware security modules market across varied regions.

Market Diversification: Exhaustive information about new solutions and services, untapped geographies, recent developments, and investments in the hardware security modules market.

Competitive Assessment: In-depth assessment of market shares, growth strategies, and solution and service offerings of leading players, including Thales (France), IBM (US), Utimaco Management Services GmbH (Germany), Futurex (US), and Entrust Corporation (US).

Contents

1 INTRODUCTION

- 1.1 STUDY OBJECTIVES
- 1.2 MARKET DEFINITION
- 1.3 STUDY SCOPE
 - 1.3.1 MARKETS COVERED AND REGIONAL SCOPE
 - 1.3.2 INCLUSIONS AND EXCLUSIONS
 - 1.3.3 YEARS CONSIDERED
- 1.4 CURRENCY CONSIDERED
- 1.5 UNIT CONSIDERED
- 1.6 STAKEHOLDERS
- 1.7 LIMITATIONS
- 1.8 SUMMARY OF CHANGES

2 RESEARCH METHODOLOGY

- 2.1 RESEARCH DATA
 - 2.1.1 SECONDARY DATA
 - 2.1.1.1 List of key secondary sources
 - 2.1.1.2 Key data from secondary sources
 - 2.1.2 PRIMARY DATA
 - 2.1.2.1 List of primary interview participants
 - 2.1.2.2 Breakdown of primaries
 - 2.1.2.3 Key data from primary sources
 - 2.1.2.4 Key industry insights
 - 2.1.3 SECONDARY AND PRIMARY RESEARCH
- 2.2 MARKET SIZE ESTIMATION METHODOLOGY
 - 2.2.1 BOTTOM-UP APPROACH
 - 2.2.1.1 Approach to arrive at market size using bottom-up analysis (demand side)
 - 2.2.2 TOP-DOWN APPROACH
 - 2.2.2.1 Approach to arrive at market size using top-down analysis (supply side)
- 2.3 MARKET BREAKDOWN AND DATA TRIANGULATION
- 2.4 RESEARCH ASSUMPTIONS
- 2.5 RISK ANALYSIS
- 2.6 RESEARCH LIMITATIONS

3 EXECUTIVE SUMMARY

4 PREMIUM INSIGHTS

4.1 ATTRACTIVE GROWTH OPPORTUNITIES FOR PLAYERS IN HARDWARE SECURITY MODULES MARKET

4.2 HARDWARE SECURITY MODULES MARKET, BY DEPLOYMENT TYPE

4.3 HARDWARE SECURITY MODULES MARKET, BY VERTICAL

4.4 HARDWARE SECURITY MODULES MARKET, BY APPLICATION

4.5 HARDWARE SECURITY MODULES MARKET, BY TYPE AND TECHNOLOGY

4.6 HARDWARE SECURITY MODULES MARKET, BY COUNTRY

5 MARKET OVERVIEW

5.1 INTRODUCTION

5.2 MARKET DYNAMICS

5.2.1 DRIVERS

5.2.1.1 Increasing data breaches and cyberattacks

5.2.1.2 Need to comply with stringent data security regulations and standards

5.2.1.3 Growing demand for effective management of cryptographic keys

5.2.1.4 Transition to digital transactions and electronic payments

5.2.1.5 Shift toward SDN and NFV in 5G deployments

5.2.2 RESTRAINTS

5.2.2.1 High ownership costs associated with hardware security modules

5.2.2.2 Susceptibility to cyberattacks and security breaches

5.2.3 OPPORTUNITIES

5.2.3.1 Rising volume of data generated by websites and mobile apps

5.2.3.2 Proliferation of connected devices and IoT technologies in smart cities

5.2.3.3 Rise of telemedicine and remote healthcare services

5.2.3.4 Increasing adoption of blockchain and cryptocurrencies

5.2.3.5 Advancements in quantum computing

5.2.4 CHALLENGES

5.2.4.1 Discovering and protecting sensitive data

5.2.4.2 Complexities associated with HSM integration process

5.2.4.3 Rise of complex IT environments

5.3 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS

5.4 PRICING ANALYSIS

- 5.4.1 AVERAGE SELLING PRICE TREND OF HSMS, BY KEY PLAYER
- 5.4.2 AVERAGE SELLING PRICE TREND OF HSMS, BY TYPE
- 5.4.3 AVERAGE SELLING PRICE TREND OF LAN-BASED/NETWORK-ATTACHED HSMS, BY REGION
- 5.5 SUPPLY CHAIN ANALYSIS
- 5.6 ECOSYSTEM ANALYSIS
- 5.7 TECHNOLOGY ANALYSIS
 - 5.7.1 KEY TECHNOLOGIES
 - 5.7.1.1 AI and ML
 - 5.7.1.2 Contactless smart cards
 - 5.7.1.3 Quantum safe hardware security modules
 - 5.7.2 COMPLEMENTARY TECHNOLOGIES
 - 5.7.2.1 PKI
 - 5.7.3 ADJACENT TECHNOLOGIES
 - 5.7.3.1 Blockchain and distributed ledger technologies
 - 5.7.3.2 Digital signatures
- 5.8 PATENT ANALYSIS
- 5.9 TRADE ANALYSIS
 - 5.9.1 IMPORT DATA (HS CODE 8471)
 - 5.9.2 EXPORT DATA (HS CODE 8471)
- 5.10 KEY CONFERENCES AND EVENTS, 2025–2026
- 5.11 CASE STUDY ANALYSIS
 - 5.11.1 EPX ACHIEVED FUTURE-PROOF PAYMENT PROCESSING INFRASTRUCTURE WITH FUTUREX'S EXCRYPT SERIES
 - 5.11.2 FORTANIX HELPED IT AND NETWORKING COMPANY WITH DSM SAAS THAT OFFERED ROBUST AND CONSISTENT SECURITY ACROSS GLOBAL OPERATIONS
 - 5.11.3 FUTUREX HELPED POMELO IMPLEMENT ROBUST CLOUD-BASED PAYMENT INFRASTRUCTURE
 - 5.11.4 STANCHION AND FUTUREX ASSISTED ISRAELI BANK WITH SECURED PAYMENT ENVIRONMENTS
 - 5.11.5 THALES LUNA HSMS HELPED BANGLADESH'S IDTP WITH ENHANCED SECURITY AND ALLOWED SECURE REAL-TIME MOVEMENT OF FUNDS
 - 5.11.6 THALES HELPED TREEZOR DEPLOY CLOUD HSM THAT PROVIDED EVERY CUSTOMER WITH EXCLUSIVE HSM SERVICE
- 5.12 INVESTMENT AND FUNDING SCENARIO
- 5.13 TARIFF AND REGULATORY LANDSCAPE
 - 5.13.1 TARIFF ANALYSIS
 - 5.13.2 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER

ORGANIZATIONS

5.13.3 STANDARDS

5.14 PORTER'S FIVE FORCES ANALYSIS

5.14.1 THREAT OF NEW ENTRANTS

5.14.2 THREAT OF SUBSTITUTES

5.14.3 BARGAINING POWER OF SUPPLIERS

5.14.4 BARGAINING POWER OF BUYERS

5.14.5 INTENSITY OF COMPETITIVE RIVALRY

5.15 KEY STAKEHOLDERS AND BUYING PROCESS

5.15.1 KEY STAKEHOLDERS IN BUYING PROCESS

5.15.2 BUYING CRITERIA

5.16 IMPACT OF AI ON HARDWARE SECURITY MODULES MARKET

6 HARDWARE SECURITY MODULES MARKET, BY TYPE

6.1 INTRODUCTION

6.2 LAN-BASED/NETWORK-ATTACHED

6.2.1 ABILITY TO PROVIDE HIGH SCALABILITY AND REMOTE ACCESS TO FUEL MARKET GROWTH

6.3 PCI-BASED/EMBEDDED PLUGINS

6.3.1 INCREASING DEMAND FOR LOW-LATENCY CRYPTOGRAPHIC PROCESSING AND HIGH-THROUGHPUT TO SUPPORT MARKET GROWTH

6.4 USB-BASED/PORTABLE

6.4.1 RISING DEMAND FOR SECURE AND PORTABLE CRYPTOGRAPHIC SOLUTIONS TO BENEFIT MARKET

6.5 SMART CARDS

6.5.1 GROWING DEMAND FOR SECURE BIOMETRIC AUTHENTICATION TO DRIVE MARKET

7 HARDWARE SECURITY MODULES MARKET, BY TECHNOLOGY

7.1 INTRODUCTION

7.2 GENERAL-PURPOSE CRYPTOGRAPHY

7.2.1 SURGING ADOPTION OF DIGITAL SERVICES AND GROWING NEED FOR DATA PROTECTION TO FOSTER MARKET GROWTH

7.3 QUANTUM CRYPTOGRAPHY

7.3.1 RISING THREATS FROM QUANTUM COMPUTING TO DRIVE MARKET

8 HARDWARE SECURITY MODULES MARKET, BY DEPLOYMENT TYPE

8.1 INTRODUCTION

8.2 ON-PREMISES

8.2.1 ABILITY TO CONTROL CRYPTOGRAPHIC KEYS AND DATA TO BOOST DEMAND

8.3 CLOUD-BASED

8.3.1 EXPANDING SECURITY DIGITAL PAYMENT ECOSYSTEMS AND E-COMMERCE PLATFORMS TO FUEL MARKET GROWTH

9 HARDWARE SECURITY MODULES MARKET, BY APPLICATION

9.1 INTRODUCTION

9.2 PAYMENT PROCESSING

9.2.1 GLOBAL SHIFT TOWARD CASHLESS ECONOMY TO FUEL MARKET GROWTH

9.3 CODE AND DOCUMENT SIGNING

9.3.1 RISING MALWARE AND SUPPLY CHAIN ATTACKS TO BOOST DEMAND

9.4 SECURITY SOCKETS LAYER (SSL) AND TRANSPORT LAYER SECURITY (TLS)

9.4.1 GROWING APPLICATION FOR PROTECTING CONFIDENTIAL DATA FOR WEB-BASED RETAIL TO BOOST DEMAND

9.5 AUTHENTICATION

9.5.1 INCREASING DEMAND FOR SECURE USER AND DEVICE AUTHENTICATION TO SUPPORT MARKET GROWTH

9.6 DATABASE ENCRYPTION

9.6.1 EXPANSION OF BIG DATA ANALYTICS TO DRIVE MARKET

9.7 PUBLIC KEY INFRASTRUCTURE (PKI) AND CREDENTIAL MANAGEMENT

9.7.1 INCREASING DEMAND FOR TAMPER-RESISTANT ENVIRONMENT FOR GENERATING, STORING, AND MANAGING CRYPTOGRAPHIC KEYS TO FOSTER MARKET GROWTH

9.8 APPLICATION-LEVEL ENCRYPTION

9.8.1 GROWING ADOPTION OF CLOUD COMPUTING, HYBRID IT ARCHITECTURES, AND DISTRIBUTED SYSTEMS TO DRIVE MARKET

10 HARDWARE SECURITY MODULES MARKET, BY VERTICAL

10.1 INTRODUCTION

10.2 BFSI

10.2.1 SURGING ADOPTION OF ADVANCED PAYMENT METHODS TO BOOST DEMAND

10.3 IT & TELECOMMUNICATIONS

10.3.1 RISING NEED TO SAFEGUARD NETWORK FUNCTION VIRTUALIZATION INFRASTRUCTURE TO FOSTER MARKET GROWTH

10.4 PUBLIC SECTOR/GOVERNMENT

10.4.1 RISING SHIFT TOWARD E-GOVERNANCE TO FUEL MARKET GROWTH

10.5 INDUSTRIAL MANUFACTURING

10.5.1 GROWING NEED TO PREVENT UNAUTHORIZED ACCESS TO DIGITAL TWIN DATA TO DRIVE MARKET

10.6 ENERGY & POWER

10.6.1 SURGING PENETRATION OF RENEWABLE ENERGY AND DISTRIBUTED ENERGY RESOURCES IN MODERN ELECTRIC GRIDS TO FUEL MARKET GROWTH

10.7 CONSUMER GOODS & RETAIL

10.7.1 INCREASING ADOPTION OF ONLINE PLATFORMS, CLOUD-BASED POINT-OF-SALE SYSTEMS, AND ADVANCED RETAIL TECHNOLOGIES TO DRIVE MARKET

10.8 MEDICAL & LIFE SCIENCES

10.8.1 SURGING ADOPTION OF ELECTRONIC HEALTH RECORDS, TELEMEDICINE, AND IOT-ENABLED MEDICAL DEVICES TO FOSTER MARKET GROWTH

10.9 AEROSPACE & DEFENSE

10.9.1 GROWING RELIANCE ON SECURED COMMUNICATIONS AND ENCRYPTED DATA TRANSMISSIONS TO SUPPORT MARKET GROWTH

10.10 TRANSPORTATION

10.10.1 INCREASING SHIFT TOWARD CONNECTED SYSTEMS, AUTONOMOUS VEHICLES, AND SMART INFRASTRUCTURE TO FOSTER MARKET GROWTH

11 HARDWARE SECURITY MODULES MARKET, BY REGION

11.1 INTRODUCTION

11.2 NORTH AMERICA

11.2.1 MACROECONOMIC OUTLOOK FOR NORTH AMERICA

11.2.2 US

11.2.2.1 Rising cybersecurity threats to foster market growth

11.2.3 CANADA

11.2.3.1 Increasing emphasis on developing and installing new network systems to accelerate demand

11.2.4 MEXICO

11.2.4.1 Thriving manufacturing hub for automotive, mining, and electronics

industries to fuel market growth

11.3 EUROPE

11.3.1 MACROECONOMIC OUTLOOK FOR EUROPE

11.3.2 GERMANY

11.3.2.1 Rising deployment of security solutions to protect production control and data exchanges to accelerate demand

11.3.3 UK

11.3.3.1 Growing need for tamper-proof encryption key management and cryptographic processing to support market growth

11.3.4 FRANCE

11.3.4.1 Increasing reliance on cloud-based solutions to drive market

11.3.5 ITALY

11.3.5.1 Government-led initiatives to improve cyber resilience to boost demand

11.3.6 REST OF EUROPE

11.4 ASIA PACIFIC

11.4.1 MACROECONOMIC OUTLOOK FOR ASIA PACIFIC

11.4.2 CHINA

11.4.2.1 Presence of stringent cybersecurity regulations to spur market growth

11.4.3 JAPAN

11.4.3.1 Increasing influx of FDIs to foster market growth

11.4.4 INDIA

11.4.4.1 Rising adoption of blockchain in BFSI, healthcare, and IT sectors to fuel market growth

11.4.5 SOUTH KOREA

11.4.5.1 Widespread adoption of 5G networks and high internet penetration to drive market

11.4.6 AUSTRALIA

11.4.6.1 Growing need to comply with cybersecurity standards and protect sensitive information to fuel market growth

11.4.7 REST OF ASIA PACIFIC

11.5 ROW

11.5.1 MACROECONOMIC OUTLOOK FOR ROW

11.5.2 SOUTH AMERICA

11.5.2.1 Expanding e-commerce market to offer lucrative growth opportunities

11.5.3 MIDDLE EAST & AFRICA

11.5.3.1 GCC

11.5.3.1.1 Rising cyberattacks in banking, government, and energy sectors to boost demand

11.5.3.2 Rest of Middle East & Africa

12 COMPETITIVE LANDSCAPE

12.1 INTRODUCTION

12.2 KEY PLAYER STRATEGIES/RIGHT TO WIN, 2020–2024

12.3 REVENUE ANALYSIS, 2020–2023

12.4 MARKET SHARE ANALYSIS, 2024

12.5 COMPANY VALUATION AND FINANCIAL METRICS, 2024

12.6 BRAND/PRODUCT COMPARISON

12.7 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2024

12.7.1 STARS

12.7.2 EMERGING LEADERS

12.7.3 PERVASIVE PLAYERS

12.7.4 PARTICIPANTS

12.7.5 COMPANY FOOTPRINT: KEY PLAYERS, 2024

12.7.5.1 Company footprint

12.7.5.2 Region footprint

12.7.5.3 Type footprint

12.7.5.4 Technology footprint

12.7.5.5 Deployment type footprint

12.7.5.6 Application footprint

12.7.5.7 Vertical footprint

12.8 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2024

12.8.1 PROGRESSIVE COMPANIES

12.8.2 RESPONSIVE COMPANIES

12.8.3 DYNAMIC COMPANIES

12.8.4 STARTING BLOCKS

12.8.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2024

12.8.5.1 Detailed list of key startups/SMEs

12.8.6 COMPETITIVE BENCHMARKING OF KEY STARTUPS/SMES

12.9 COMPETITIVE SCENARIO

12.9.1 PRODUCT LAUNCHES/DEVELOPMENTS

12.9.2 DEALS

12.9.3 EXPANSIONS

12.9.4 OTHER DEVELOPMENTS

13 COMPANY PROFILES

13.1 KEY PLAYERS

13.1.1 THALES

13.1.1.1 Business overview

13.1.1.2 Products/Solutions/Services offered

13.1.1.3 Recent developments

13.1.1.3.1 Product launches/Developments

13.1.1.3.2 Deals

13.1.1.4 MnM view

13.1.1.4.1 Key strengths/Right to win

13.1.1.4.2 Strategic choices

13.1.1.4.3 Weaknesses/Competitive threats

13.1.2 UTIMACO MANAGEMENT SERVICES GMBH

13.1.2.1 Business overview

13.1.2.2 Products/Solutions/Services offered

13.1.2.3 Recent developments

13.1.2.3.1 Product launches/Developments

13.1.2.3.2 Deals

13.1.2.3.3 Expansions

13.1.2.4 MnM view

13.1.2.4.1 Key strengths/Right to win

13.1.2.4.2 Strategic choices

13.1.2.4.3 Weaknesses/Competitive threats

13.1.3 FUTUREX

13.1.3.1 Business overview

13.1.3.2 Products/Solutions/Services offered

13.1.3.3 Recent developments

13.1.3.3.1 Product launches/Developments

13.1.3.3.2 Deals

13.1.3.4 MnM view

13.1.3.4.1 Key strengths/Right to win

13.1.3.4.2 Strategic choices

13.1.3.4.3 Weaknesses/Competitive threats

13.1.4 IBM

13.1.4.1 Business overview

13.1.4.2 Products/Solutions/Services offered

13.1.4.3 Recent developments

13.1.4.3.1 Deals

13.1.4.4 MnM view

13.1.4.4.1 Key strengths/Right to win

13.1.4.4.2 Strategic choices

- 13.1.4.4.3 Weaknesses/Competitive threats
- 13.1.5 ENTRUST CORPORATION
 - 13.1.5.1 Business overview
 - 13.1.5.2 Products/Solutions/Services offered
 - 13.1.5.3 Recent developments
 - 13.1.5.3.1 Product launches/Developments
 - 13.1.5.3.2 Deals
 - 13.1.5.3.3 Expansions
 - 13.1.5.4 MnM view
 - 13.1.5.4.1 Key strengths/Right to win
 - 13.1.5.4.2 Strategic choices
 - 13.1.5.4.3 Weaknesses/Competitive threats
- 13.1.6 ATOS SE
 - 13.1.6.1 Business overview
 - 13.1.6.2 Products/Solutions/Services offered
 - 13.1.6.3 Recent developments
 - 13.1.6.3.1 Product launches/Developments
 - 13.1.6.3.2 Deals
- 13.1.7 STMICROELECTRONICS
 - 13.1.7.1 Business overview
 - 13.1.7.2 Products/Solutions/Services offered
 - 13.1.7.3 Recent developments
 - 13.1.7.3.1 Deals
- 13.1.8 MICROCHIP TECHNOLOGY INC.
 - 13.1.8.1 Business overview
 - 13.1.8.2 Products/Solutions/Services offered
 - 13.1.8.3 Recent developments
 - 13.1.8.3.1 Product launches/Developments
 - 13.1.8.3.2 Deals
 - 13.1.8.3.3 Other developments
- 13.1.9 INFINEON TECHNOLOGIES AG
 - 13.1.9.1 Business overview
 - 13.1.9.2 Products/Solutions/Services offered
 - 13.1.9.3 Recent developments
 - 13.1.9.3.1 Product launches/Developments
 - 13.1.9.3.2 Deals
- 13.1.10 YUBICO
 - 13.1.10.1 Business overview
 - 13.1.10.2 Products/Solutions/Services offered

- 13.1.10.3 Recent developments
 - 13.1.10.3.1 Product launches/Developments
 - 13.1.10.3.2 Deals
- 13.1.11 DINAMO NETWORKS
 - 13.1.11.1 Business overview
 - 13.1.11.2 Products/Solutions/Services offered

13.2 OTHER PLAYERS

- 13.2.1 SECUROSYS
- 13.2.2 SPYRUS
- 13.2.3 ADWEB TECHNOLOGIES
- 13.2.4 LATTICE SEMICONDUCTOR
- 13.2.5 ELLIPTICSECURE
- 13.2.6 AMAZON WEB SERVICES, INC.
- 13.2.7 ETAS
- 13.2.8 SANSEC
- 13.2.9 FORTANIX
- 13.2.10 JISA SOFTECH PVT. LTD.
- 13.2.11 MICROSOFT
- 13.2.12 NITROKEY
- 13.2.13 KRYPTOAGILE SOLUTIONS PVT. LTD.
- 13.2.14 KRYPTUS
- 13.2.15 CRYPTO4A

14 APPENDIX

- 14.1 INSIGHTS FROM INDUSTRY EXPERTS
- 14.2 DISCUSSION GUIDE
- 14.3 KNOWLEDGESTORE: MARKETSandMARKETS' SUBSCRIPTION PORTAL
- 14.4 CUSTOMIZATION OPTIONS
- 14.5 RELATED REPORTS
- 14.6 AUTHOR DETAILS

I would like to order

Product name: Hardware Security Modules Market by Technology (General Purpose Cryptography, Quantum Cryptography), Type (LAN Based /Network Attached, PCI Based/Embedded Plugins, USB Based, Smart Cards), Deployment Type (Cloud, On-premise) - Global Forecast to 2030

Product link: <https://marketpublishers.com/r/HF28ACE291B3EN.html>

Price: US\$ 4,950.00 (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/HF28ACE291B3EN.html>