+357 96 030922
info@marketpublishers.com

Embedded Systems Security Hardware Market Forecasts to 2034 – Global Analysis By Hardware Type (Secure Elements (SEs), Trusted Platform Modules (TPMs), Hardware Security Modules (HSMs), Cryptographic Accelerators and Secure Microcontrollers (MCUs)), Security Function, Application, End User and By Geography

https://marketpublishers.com/r/EA1B81DAC1C7EN.html
Date: May 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: EA1B81DAC1C7EN

Abstracts

According to Stratistics MRC, the Global Embedded Systems Security Hardware Market is accounted for $14.8 billion in 2026 and is expected to reach $29.3 billion by 2034 growing at a CAGR of 8.9% during the forecast period. Embedded Systems Security Hardware consists of dedicated physical security components that safeguard embedded devices against cyberattacks, unauthorized entry, and data leaks. It includes technologies such as secure elements, TPMs, hardware security modules, and encryption accelerators that enable secure boot processes, data encryption, authentication, and integrity checks. These solutions are commonly applied in automotive electronics, industrial control systems, healthcare devices, and IoT networks. By handling security functions at the hardware level instead of software, they enhance efficiency and improve resistance to hacking attempts. With rising connectivity in embedded systems, such hardware is essential for protecting data and ensuring dependable system operation.

According to PSA Certified, over 500 million devices have been deployed with PUF (Physically Unclonable Function)-enabled hardware security primitives, providing device authentication and resistance against cloning attacks. PSA Level 3 certified components are now commercially available, ensuring hardware Roots of Trust in embedded systems.

Market Dynamics:

+357 96 030922
info@marketpublishers.com

Driver:

Increasing cybersecurity threats and attacks

The rise in advanced cyber threats is significantly driving the need for embedded systems security hardware. Attackers are increasingly focusing on embedded devices used in critical areas such as financial systems, healthcare devices, industrial machinery, and automotive electronics. Traditional software security measures often fail to defend against complex attacks like firmware manipulation and hardware-level exploits. As a result, there is growing reliance on hardware-based security technologies that offer stronger protection and isolation. These solutions support secure booting, data encryption, and resistance to tampering, ensuring embedded systems can better withstand sophisticated cyberattacks in today's highly connected digital landscape.

Restraint:

High implementation and integration costs

The high cost associated with implementing and integrating embedded security hardware significantly restricts market growth. Security technologies like secure elements, hardware security modules, and trusted platform modules require substantial investment during development and production. Integrating these components into existing embedded systems also increases technical complexity and overall expenses. Smaller companies, in particular, find it difficult to adopt such costly solutions due to financial limitations. In addition, expenses related to testing, certification, and regulatory compliance further increase the total cost. Consequently, many cost-sensitive organizations either postpone or reduce the adoption of advanced embedded hardware security technologies.

Opportunity:

Increasing adoption of edge computing

The rising use of edge computing presents a strong opportunity for growth in the embedded systems security hardware market. Edge devices handle data processing near the source, enabling faster responses in sectors like healthcare, manufacturing, and communication networks. However, these devices often function in remote or less protected environments, increasing their exposure to cyber risks. Hardware-based security solutions help safeguard these systems through encryption technologies, secure authentication methods, and protected key management. As more industries adopt decentralized computing architectures, the need for secure edge infrastructure is growing, creating substantial opportunities for embedded security hardware providers.

Threat:

High dependence on semiconductor supply chain

A strong threat to the embedded systems security hardware market is its reliance on the global semiconductor supply chain. Security hardware depends on advanced chips produced by a small group of manufacturers located in specific regions. Any disruptions

+357 96 030922
info@marketpublishers.com

such as geopolitical conflicts, trade barriers, natural disasters, or manufacturing shortages can severely affect supply availability. These issues often result in production delays, higher costs, and limited access to essential components. Because the supply base is not widely diversified, the market remains highly exposed to external disruptions, making it difficult for companies to consistently meet rising demand for embedded security solutions.

Covid-19 Impact:

The COVID-19 outbreak created both challenges and growth opportunities for the embedded systems security hardware market. In the early stages, manufacturing disruptions, supply chain breakdowns, and semiconductor shortages led to delayed production and reduced hardware availability. Many organizations also cut back on spending, temporarily slowing market growth. However, the pandemic significantly accelerated digital adoption, remote connectivity, and the use of IoT and cloud-based systems. This increased reliance on connected infrastructure raised cybersecurity risks, driving higher demand for embedded security hardware. Industries like healthcare, telecom, and industrial automation strengthened their investments in secure systems to maintain data protection and operational continuity during the crisis.

The secure elements (SEs) segment is expected to be the largest during the forecast period

The secure elements (SEs) segment is expected to account for the largest market share during the forecast period because they are widely adopted in consumer electronics, IoT devices, and mobile platforms. These secure chips are built to resist tampering and are used to safely store encryption keys, credentials, and sensitive information. Their small form factor, energy efficiency, and affordability make them ideal for integration into various embedded applications. SEs are commonly found in smart phones, smart payment cards, and connected devices, where strong data protection is essential. Due to their versatility and ease of deployment, they maintain the leading position among different embedded security hardware solutions.

The connected automotive systems segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the connected automotive systems segment is predicted to witness the highest growth rate. This growth is driven by increasing vehicle connectivity and advancements in autonomous driving technologies. Today’s vehicles depend heavily on embedded systems for functions such as navigation, entertainment, communication, and V2X connectivity. As connectivity increases, so does the risk of cyber attacks, making hardware-based security solutions essential. Technologies like secure microcontrollers, encryption modules, and hardware security components are being widely adopted in the automotive sector. The rapid shift toward electric and self-driving vehicles is further accelerating demand and boosting strong growth in this

+357 96 030922
info@marketpublishers.com

segment.
Region with largest share:
During the forecast period, the North America region is expected to hold the largest market share because of its advanced technological ecosystem and strong cyber security adoption. The region is supported by major semiconductor manufacturers and leading security hardware providers. High investments in IoT, automotive electronics, aerospace, defence, and industrial automation further strengthen demand for embedded security solutions. Strict regulatory frameworks and data protection laws encourage the use of secure hardware technologies. The rapid expansion of connected devices and cloud infrastructure increases the need for strong security measures. Continuous innovation and the presence of key industry players accelerate the deployment of advanced embedded security hardware across various sectors.
Region with highest CAGR:
Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR. This is driven by rapid industrial growth, strong electronics manufacturing capabilities, and widespread adoption of IoT and smart technologies. Key countries like China, India, Japan, and South Korea are investing heavily in automotive systems, consumer electronics, and industrial automation. Increasing digital transformation and rising awareness of cybersecurity risks are boosting demand for secure embedded hardware. The region also benefits from a strong semiconductor production ecosystem and cost advantages. Government support for smart cities and digital infrastructure further accelerates market expansion across Asia Pacific.
Key players in the market
Some of the key players in Embedded Systems Security Hardware Market include Infineon Technologies, NXP Semiconductors, STMicroelectronics, Qualcomm, Microchip Technology, Renesas Electronics, Arm Holdings, Texas Instruments, Broadcom, Thales Group, Samsung Electronics, HID Global, SecureRF, Onsemi, Spyrus, Rambus, IDEMIA and Intel Corp.
Key Developments:
In April 2026, Intel Corp plans to invest an additional $15 million in AI chip startup SambaNova Systems, according to a Reuters review of corporate records, as the semiconductor company deepens its focus on artificial intelligence infrastructure. The proposed investment, which is subject to regulatory approval, would raise Intel’s ownership stake in SambaNova to approximately 9%.
In February 2026, STMicroelectronics (STM) unveiled an expanded multi-year, multi-billion-dollar collaboration with Amazon Web Services (AMZN), spanning multiple product lines, including a warrant issuance to AWS for up to 24.8 million ST shares. The collaboration establishes STMicroelectronics (STM) as a strategic supplier of advanced semiconductor technologies and products that AWS integrates into its compute

+357 96 030922
info@marketpublishers.com

infrastructure.
In January 2026, Qualcomm Technologies, Inc. and Hyundai Mobis announced that the companies have signed a comprehensive agreement at CES 2026 to co-develop next-generation solutions for Software-Defined Vehicles (SDV) and Advanced Driver Assistance Systems (ADAS). Through this collaboration, Hyundai Mobis and Qualcomm Technologies will jointly develop integrated solutions tailored for emerging markets.
Hardware Types Covered:

- Secure Elements (SEs)
- Trusted Platform Modules (TPMs)
- Hardware Security Modules (HSMs)
- Cryptographic Accelerators
- Secure Microcontrollers (MCUs)

Security Functions Covered:

- Authentication & Access Control
- Payment & Transaction Security
- Content Protection
- Data Encryption & Key Management

Applications Covered:

- IoT Devices
- Connected Automotive Systems
- Medical Devices
- Consumer Electronics

+357 96 030922
info@marketpublishers.com

- Aerospace & Defense Systems

End Users Covered:

- Automotive OEMs & Tier-1 Suppliers
- Healthcare Providers & Medical Equipment Manufacturers
- Consumer Electronics Manufacturers
- Telecommunications Operators & Network Equipment Vendors
- Industrial Automation & Manufacturing Enterprises
- Aerospace & Defense Contractors

Regions Covered:

- North America
  - United States
  - Canada
  - Mexico
- Europe
  - United Kingdom
  - Germany
  - France
  - Italy

+357 96 030922
info@marketpublishers.com

- 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

+357 96 030922
info@marketpublishers.com

- 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:

+357 96 030922
info@marketpublishers.com

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

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

9 GLOBAL EMBEDDED SYSTEMS SECURITY HARDWARE MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

10 STRATEGIC MARKET INTELLIGENCE

11 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

12 COMPANY PROFILES

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+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: Embedded Systems Security Hardware Market Forecasts to 2034 – Global Analysis By Hardware Type (Secure Elements (SEs), Trusted Platform Modules (TPMs), Hardware Security Modules (HSMs), Cryptographic Accelerators and Secure Microcontrollers (MCUs)), Security Function, Application, End User and By Geography

Product link: https://marketpublishers.com/r/EA1B81DAC1C7EN.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/EA1B81DAC1C7EN.html