Embedded Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Embedded Security Market size is estimated at USD 8.85 billion in 2025, and is expected to reach USD 12.05 billion by 2030, at a CAGR of 6.37% during the forecast period (2025-2030).

The increasing need for embedded security solutions in various applications, such as wearables, smartphones and tablets, automotive, smart identity cards, industrial, payment processing and cards, and computers, is driving the growth of this market. Furthermore, the burgeoning Bring Your Own Device (BYOD) trend is boosting global demand for embedded security solutions.

Key Highlights

- Embedded security is implemented to safeguard the processing and cardholder data. The usage of embedded security serves to reduce the danger of data breaches, which can result in financial losses and reputational damage. It also aids in meeting the criteria of the Payment Card Industry Data Security Standard (PCI DSS). Secure elements, Trusted Execution Environment (TEE), and tamper-resistant hardware are examples of embedded security used in payment processing and cards. These embedded security solutions prevent cardholder data from being compromised by attackers, among other things.
- Technology is advancing faster than ever before. Every day, technology advances and introduces new approaches and functions. It is not just about computers and mobile applications. It is all about artificial intelligence and IoT-based gadgets, widely employed in everyday human life. The rise of IoT is spreading across all industries as it is utilized in various applications, including industrial automation, healthcare equipment, aviation, wearable technologies, smart home units, and automobiles. The growing use of IoT raises the possibility of different security vulnerabilities with connected devices. This also raises the likelihood of external cyber threats attacking running systems, causing the device to malfunction and cause harm. Also, embedded security devices are on the rise to avoid this condition.
- The market for electric vehicles is constantly evolving and maturing. Customers are aggressively seeking vehicles that do not

use traditional fossil fuels. These vehicles should be both cost-effective and environmentally beneficial. Also, to meet these needs, an increasing number of electric charging stations must be established in homes and roadways. The security of charging stations is vital to protect its critical infrastructure. The complicated design and multiple safety concerns in electric vehicles and charging points make managing all security challenges in the system tough. Embedded device security systems help with this problem. Electric vehicle security is critical due to the rising number of embedded and connected software in cars.

- These systems have gained popularity in recent years. However, the basic cost of a single physical security device plus a communication security device is more than the cost of a traditional security system. Internal components like transmitters, receivers, and sensors utilized in security systems are more expensive, directly impacting the system's primary selling price. Furthermore, renewing existing security systems and adopting new integrated technology is not cost-viable for SME enterprises and individual users.
- However, the software itself cannot ensure the security of embedded systems, no matter how sophisticated and security aware. Cloud, software, and hardware vendors must collaborate. For instance, on-chip security features allow robust key management and encryption, which is too computationally demanding for embedded software alone, and hardware technologies secure device boot integrity. Functions like path space control, rootless execution, encrypted file systems, access control rules, and threat-level anomaly detection are made feasible by hardware capabilities and installed in the operating system.

Embedded Security Market Trends

Increasing Adoption of Wearable Devices in Healthcare Expected to Drive the Market

- According to Gallup's annual Health and Healthcare survey, 90% of US consumers said they are currently using a wearable fitness tracker, and the same percentage stated that they currently use a mobile health application. Also, with the rise in national health expenditure in the United States, by combining the present use with the percentages of US citizens that claim, in the past, they have used such devices, it becomes clear that at some point, one in three citizens used a fitness tracker such as a wristband or smartwatch (34%) or tracked their health statistics on the phone or tablet application (32%).
- The majority of wearables collect and filter data directly from the wearer's body or from the environment around them using a range of sensors and other technologies. Certain wearables have the ability to process and analyze data locally, giving users instant access to results or alarms. Others are unable to process data at the source due to the small size of the sensors and storage devices. Rather, they will send the information to a smartphone, cloud app, or distant computer over Bluetooth or Wi-Fi.
- Following the analysis and parsing of data, the wearer will receive actionable insights via their smartphone application or the wearable device itself. Usually, proprietary servers in a data center or cloud will be used to keep original data and analytic results indefinitely. Due to their ability to facilitate communication between sensors and control systems, communication networks are essential to the success of wearable technology. With decreased end-to-end latency, these networks are growing quicker and more capable of supporting sophisticated wearables with the advent of 5G technology.
- According to a study published in Nature Medicine, wearable fitness trackers were designed to detect COVID-19 by building a system that detected 80% of pre-symptomatic and asymptomatic infections. The study involved more than 3,300 adults aged 18-80 who installed the researchers' app, called MyPHD, on their Android or Apple devices. The app collected data from the wearables they already had and transferred it to a secure cloud server where the researchers could analyze the data. The wearables included Fitbits, Apple Watches, Garmin devices, and other gadgets compatible with either Apple's HealthKit or the Google Fit platforms.
- Further, technology services firm Vee Technologies and Sona Group of educational institutions recently signed an agreement with Toronto-based University Health Network (UHN) to develop smart fabric-based wearables. This initiative will help develop smart textiles and garments that can support the growing needs of the healthcare industry in Canada. The collaboration agreement seeks to contribute to FIBRE, a research initiative by The University Health Network (UHN), a public research and teaching hospital.

North America Accounts for a Significant Market Share

- North America accounts for a significant share of the embedded security market, as growing concerns for protecting critical infrastructure and sensitive data have increased interventions by regional government bodies in recent years. Thus, government initiatives, such as specific budget allocations and mandated security policies, are expected to drive the market of embedded security in North America.
- The proliferation of IoT devices promises to improve infrastructure efficiency, ease of monitoring, and quality of life, but it also poses new security threats. In the IoT landscape, all smart gadgets are by nature Internet-connected, with the data they generate and utilize kept on servers that are vulnerable to hacking. These factors make embedded security necessary.
- The use of sensors integrated into security-embedded hardware can vary based on the industry in which a specific company operates. For instance, drones can be used to inspect big expanses of land if end users are cultivating crops. IoT devices can assist in locating each shipment in a fleet of trucks and in estimating the time it will take to reach its destination. If end users run a manufacturing plant, they can use linked IoT sensors to determine whether a specific piece of equipment needs repair or to find out how efficient the assembly line is with the help of embedded security solutions.
- To protect their system from intrusions, dealerships and Cars.com implemented a two-step login process. According to Helion Technologies, several insurers need it as a requirement for dealership cybersecurity coverage. Further, the new budget spending for Canadian infrastructure protection is marked at USD 144.9 million over five years, including Canada's critical cyber systems, which span the finance, telecommunications, energy, and transport industries, further driving the demand for embedded security solutions.
- The Health Insurance Portability and Accountability Act, a federal statute of the United States, reported an increase of 25% annually in data breaches in the Healthcare Data Breach Report, with 29,298,012 healthcare records in total breached. Such increases are projected to drive the market studied.

Embedded Security Industry Overview

The embedded security market is highly fragmented, and major players have used various strategies, such as new product launches, expansions, agreements, partnerships, and acquisitions, to increase their footprints in this market. Such developments result in an intense rivalry in the market. Key players include Infineon Technologies AG and STMicroelectronics NV.

In March 2024, Monta Vista Software LLC, a company offering commercial embedded Linux solutions, announced the release of CG X 5.0. This significant 15th iteration of the carrier-grade Linux product line highlights Monta Vista's dedication to secure dependable and creative embedded systems development by introducing a number of advanced security improvements and updates.

In February 2024, LDRA, the leading inventor in embedded systems and technology, announced the much-anticipated return of the embedded safety and security summit (ESSS) as a physical event across India during the month of July 2024.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

1 INTRODUCTION
1.1 Study Deliverables
1.2 Study Assumptions
1.3 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET DYNAMICS
4.1 Market Overview
4.2 Market Drivers
4.2.1 Growing IoT Applications Increasing the Need for IoT Security
4.2.2 Adoption of Wearable Devices in Healthcare
4.3 Market Restraints
4.3.1 Low Demand Due to Impact of COVID-19
4.3.2 Non-adherence to Government Regulations Due to Lack of Auditing
4.4 Industry Value Chain Analysis
4.5 Industry Attractiveness - Porter's Five Forces
4.5.1 Threat of New Entrants
4.5.2 Bargaining Power of Buyers/Consumers
4.5.3 Bargaining Power of Suppliers
4.5.4 Threat of Substitute Products
4.5.5 Intensity of Competitive Rivalry

5 MARKET SEGMENTATION
5.1 Component Type
5.1.1 Hardware
5.1.2 Software
5.1.3 Service
5.2 Application
5.2.1 Payment
5.2.2 Authentication
5.2.3 Content Protection
5.2.4 Other Applications
5.3 End User
5.3.1 Automotive
5.3.2 Healthcare
5.3.3 Consumer Electronics
5.3.4 Telecommunications
5.3.5 Aerospace & Defence
5.3.6 Other End Users
5.4 Geography
5.4.1 North America
5.4.1.1 United States
5.4.1.2 Canada
5.4.2 Europe

5.4.2.1 Germany
5.4.2.2 United Kingdom
5.4.2.3 France
5.4.2.4 Rest of Europe
5.4.3 Asia-Pacific
5.4.3.1 India
5.4.3.2 China
5.4.3.3 Japan
5.4.3.4 Rest of Asia-Pacific
5.4.4 Rest of the World
5.4.4.1 Latin America
5.4.4.2 Middle East and Africa

6 COMPETITIVE LANDSCAPE
6.1 Company Profiles
6.1.1 Infineon Technologies AG
6.1.2 STMicroelectronics NV
6.1.3 Texas Instruments Inc.
6.1.4 McAfee LLC
6.1.5 Microchip Technology Inc.
6.1.6 Intellias Ltd
6.1.7 Karamba Security Ltd
6.1.8 Samsung Electronics Co.
6.1.9 Idemia Group
6.1.10 Rambus Incorporated

7 INVESTMENT ANALYSIS

8 MARKET OPPORTUNITIES AND FUTURE TRENDS

Embedded Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

□ - Print this form

□ - Complete the relevant blank fields and sign

□ - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

□** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*

Phone*

First Name*

Last Name*

Job title*

Company Name*

EU Vat / Tax ID / NIP number*

Address*

City*

Zip Code*

Country*

Date 2026-03-05

Signature