

Embedded Security Market Analysis, Industry to Expand at a 10.28% CAGR Through 2035

Embedded Security Market Size, Share and Research Report By Application (Consumer Electronics, Automotive, Industrial, Healthcare, Telecommunications)

BERLIN, BERLIN, GERMANY, June 17, 2026 /EINPresswire.com/ -- The global [Embedded Security Market](#) is

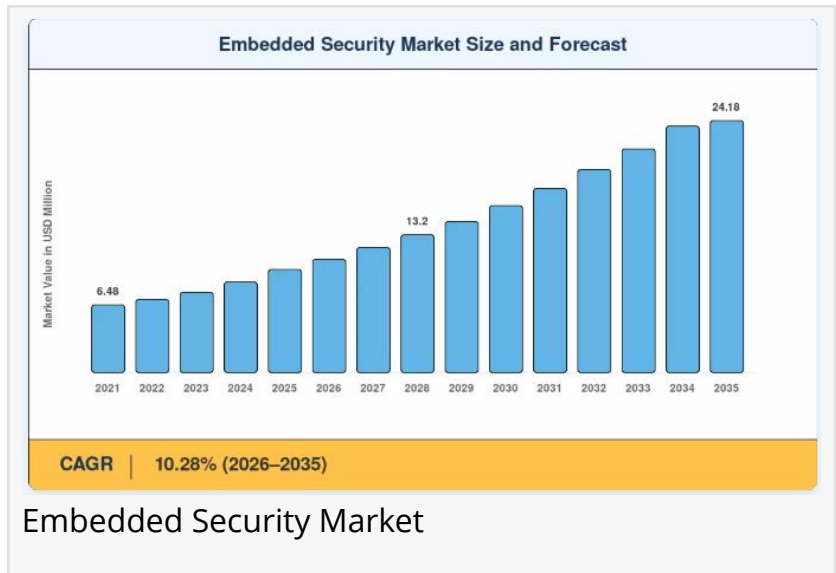
undergoing a massive transformation, driven by an increasing corporate desire for hardware-backed digital protection, immersive real-time threat monitoring, and smart asset tracking

across connected enterprise landscapes. Blending advanced cryptographic logic with predictive risk modeling and Internet of Things (IoT) connectivity, the market is poised for explosive growth over the next decade.

“

Embedded Security Market is witnessing strong growth driven by increasing cybersecurity concerns, IoT adoption, and the need for secure hardware and software protection in connected devices.”

*Market Research Future
(MRFR)*



The global Embedded Security Market size is expected to surge from its foundational base, mimicking the rapid scaling seen in cloud and semiconductor platforms, as it rides a wave of steady Compound Annual Growth Rate (CAGR) in specific cyber defense hardware segments and an overall robust CAGR in digital parametric software integration. The embedded security market reached an estimated USD 9.92 billion in 2025 and is forecast to climb from USD 10.86 billion in 2026 to USD 24.18 billion by 2035, registering a CAGR of 10.28% across the forecast window.

Get Full PDF Sample Copy of Report: (Including Full TOC,

List of Tables & Figures, Chart) @

https://www.marketresearchfuture.com/sample_request/34804

□ Key Drivers Fueling Market Growth

The convergence of three distinct technological and regulatory pillars is accelerating the expansion of the embedded security market:

Regulatory Mandates & Hardware Root of Trust Adoption: The EU Cyber Resilience Act, finalized in late 2024, mandates that by 2027, all connected products sold in Europe roughly 15.6 billion units per year embed a hardware root of trust for IoT devices. Simultaneously, UNECE Regulation 155 requires automakers to demonstrate [cybersecurity](#) management systems across the entire vehicle lifetime. These regulations shorten procurement cycles and expand the addressable embedded security market by an estimated USD 1.9 billion through 2028 by converting chip-level safeguards from a value-add into a mandatory compliance requirement.

Automotive Electrification Expanding the Attack Surface: Modern battery-electric vehicles contain 80–120 electronic control units (ECUs), roughly triple the count of legacy internal-combustion platforms. Each ECU requires secure boot and firmware signing for embedded systems to prevent over-the-air update tampering. Continental AG alone reported embedding cryptographic acceleration across 47 million ECUs shipped in 2024. This silicon-content expansion makes automotive the largest single vertical for the embedded security market, holding a 34.7% share of 2025 demand, underpinned by ARM TrustZone for embedded security in vehicle-to-everything (V2X) communication.

FIDO Passkeys, eSIM Provisioning & Post-Quantum Cryptography: According to the FIDO Alliance, by Q4 2024, there were 12 billion passkey-enabled accounts worldwide, all requiring hardware-backed credential storage. GSMA eSIM customer activations surpassed 1.2 billion in 2024, necessitating hardware security modules for on-device secure provisioning. Furthermore, NIST's finalization of CRYSTALS-Kyber and CRYSTALS-Dilithium post-quantum cryptography standards in 2024 triggered early procurement of PQC-capable secure elements by silicon vendors including Infineon and NXP, representing a long-term embedded security market growth vector.

□ Market Segmentation Analysis

To provide a granular understanding of the landscape, global market research highlights a comprehensive segmentation across several key domains:

By Component

Hardware: Maintained a 53.1% share in 2025, reflecting strong demand for secure elements, Trusted Platform Modules (TPMs), and hardware security modules for IoT integration.

Software: Includes cryptographic libraries, secure OS environments, and embedded firmware management frameworks that complement hardware-layer defenses.

Services: Recorded the highest segment CAGR at 12.34% through 2035, driven by managed security provisioning and lifecycle firmware management offerings.

□ By Application

Consumer Electronics: Leverages embedded security for biometric authentication, secure payment, and personal data protection across smartphones, wearables, and smart home devices.

Automotive: The dominant application vertical, holding a 34.7% share of 2025 demand, utilizing secure boot and firmware signing to protect V2X communications and ECU integrity.

Industrial & Healthcare: Healthcare is forecast to expand at a CAGR of 11.02% through 2035, driven by regulatory requirements for medical device security and patient data protection.

By Deployment Type

Cloud-Based: Led the segment with USD 6.24 billion in 2025 revenue, as enterprises scaled elastic HSM instances for cryptographic acceleration in embedded processors.

On-Premises: Growing at an 8.76% CAGR, fueled by data-localization statutes requiring local secure element provisioning across financial and government sectors.

Get access to the full description of the report @

<https://www.marketresearchfuture.com/reports/embedded-security-market-34804>

□ Regional Insights

Asia-Pacific: Asia-Pacific commands the dominant market share at approximately 43.6% of 2025 revenue, anchored by semiconductor fabrication capacity in Taiwan, South Korea, and mainland China. Rapid enterprise digitization and massive government-backed digital resilience initiatives across technologically intensive commercial hubs continue fueling this region's leadership position.

Europe: Europe holds the second-largest share at roughly 26% of global revenue, where regulatory mandates—particularly the EU Cyber Resilience Act and UNECE R155—continue to drive embedded security market adoption across automotive and industrial verticals, shortening procurement cycles and mandating hardware root of trust compliance.

Middle East & Africa: The Middle East & Africa region is the fastest-growing geography, registering a projected CAGR of 12.44% through 2035, propelled by smart-city initiatives in Saudi Arabia and the UAE, alongside expanding industrial IoT deployments across emerging digital

infrastructure projects.

North America: North America maintains a strong market presence sustained by high cybersecurity tech adoption rates, robust FIDO passkey and eSIM provisioning activity, and advanced telemetry-driven risk management models embedded across enterprise and government infrastructure frameworks.

□ Top Key Companies:

The global landscape is highly consolidated around critical semiconductor vendors, system integrators, and specialized security chip providers, which include:

□Infineon Technologies: A dominant silicon leader pioneering hardware security modules for IoT and PQC-ready secure elements across automotive, industrial, and consumer segments globally.

□NXP Semiconductors: A global semiconductor leader combining sophisticated secure element architectures with automotive-grade embedded security frameworks to serve connected vehicle and smart device ecosystems.

□STMicroelectronics: A major embedded security provider delivering integrated cryptographic processors and ARM TrustZone-enabled microcontrollers across industrial and consumer electronics platforms.

□Qualcomm: A pioneer integrating hardware-backed security into mobile and IoT chipsets, supporting FIDO passkey provisioning and secure device authentication at billion-unit scale.

□Microchip Technology: An international specialist bringing CryptoAuthentication and Trust Platform solutions to SMB and enterprise embedded systems requiring scalable hardware root of trust deployments.

□Samsung Electronics: A leading innovator combining secure enclave design with advanced semiconductor fabrication to deliver eSIM and payment-grade embedded security across consumer and enterprise verticals.

□Texas Instruments: An international carrier bringing expansive cryptographic hardware and secure boot frameworks to protect industrial automation and medical device assets against modern cyber threats.

□Munich Re: A major global reinsurance engine combining digital infrastructure analytics with extensive historical incident data to back large-scale embedded cyber risk exposures.

□ Emerging Trends and Future Outlook

The future of the embedded security market lies in the breakdown of silos between macro-threat modeling and micro-device level silicon design. Industry leaders are focusing on creating cohesive digital environments where an OEM or enterprise operator doesn't just purchase a secure element, but continuously generates system telemetry data via connected endpoints to optimize their next security deployment cycle. This data simultaneously allows silicon vendors to refine predictive simulation models and proactively push protective firmware alerts before a major zero-day exploit strikes.

As post-quantum cryptography standards and Secure-Element-as-a-Service models continue to merge with decentralized IoT frameworks, automated transmission of asset boundaries, historical device uptime, and verifiable breach indicators will become standard benchmarks—ensuring that the embedded security market remains highly accurate, fast-responding, and structurally resilient against global cyber threats.

□ FAQs

Q – How do continuous security monitoring tools affect the total addressable market for embedded security?

Ans – Automated digital risk-tracking and continuous monitoring solutions lower the hardware evaluation barriers for enterprise IoT networks by 40% to 60%, removing immediate verification friction. Over a multi-year horizon, this proactive technology deployment vastly expands market penetration, enabling budget-constrained organizations to adopt progressive embedded security frameworks they otherwise would avoid due to high implementation complexity.

Q – What core methodologies should silicon vendors verify before deploying post-quantum cryptography hardware modules?

Ans – Vendors must analyze historical systemic failure rates, simulate device breach outcomes against shifting international exploit baselines, and rigorously test for interoperability risk—the variance between automated sensor-reported telemetry and the actual real-world device interruption losses sustained on the ground. Compliance with NIST's finalized PQC standards and alignment with FIDO2 attestation frameworks are also non-negotiable prerequisites.

□□□ Top Industry Reports from Market Research Future:

Oled Microdisplay Market-

<https://www.marketresearchfuture.com/reports/oled-microdisplay-market-7479>

Flexible Heater Market-

<https://www.marketresearchfuture.com/reports/flexible-heater-market-7535>

Delivery Robots Market-

<https://www.marketresearchfuture.com/reports/delivery-robots-market-7551>

Ingaas Image Sensor Market-

<https://www.marketresearchfuture.com/reports/ingaas-image-sensors-market-7627>

Microprinting Market-

<https://www.marketresearchfuture.com/reports/microprinting-market-7678>

Portable Spectrometer Market-

<https://www.marketresearchfuture.com/reports/portable-spectrometer-market-7728>

3D Semiconductor Packaging Market-

<https://www.marketresearchfuture.com/reports/3d-semiconductor-packaging-market-7748>

Automatic Number Plate Recognition Market-

<https://www.marketresearchfuture.com/reports/automatic-number-plate-recognition-market-7763>

Power Supply In Package And Power Supply On Chip Market-

<https://www.marketresearchfuture.com/reports/power-supply-in-package-chip-market-7764>

Edge Ai Hardware Market-

<https://www.marketresearchfuture.com/reports/edge-ai-hardware-market-7836>

Sagar Kadam

Market Research Future

+ +1 628-258-0071

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/920129411>

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.

© 1995-2026 Newsmatics Inc. All Right Reserved.