Connected Car Security Market by Type (Endpoint, Application, Network, Security), Solution (Software & Hardware), Application (TCU, Infotainment, ADAS, Communication Modules), Form (In-vehicle, External Cloud), EV Type & Region - Global Forecast to 2032

Market Report | 2025-12-05 | 278 pages | MarketsandMarkets

AVAILABLE LICENSES:

- Single User $4950.00
- Multi User $6650.00
- Corporate License $8150.00
- Enterprise Site License $10000.00

Report description:

The connected car security market is projected to grow from USD 3.37 billion in 2025 to reach USD 6.99 billion by 2032, at a CAGR of 11.0% from 2025 to 2032. Market growth is driven by the rapid expansion of software-defined vehicles (SDVs), over-the-air (OTA) update capabilities, V2X communication, and the rising cybersecurity threats targeting vehicle ECUs, telematics units, and cloud platforms. Additionally, regulations such as UNECE WP.29 CSMS, ISO/SAE 21434, the US NHTSA cybersecurity guidelines, and China's Automotive Data Security Regulations are pushing automakers to adopt secure gateways, IDS/IPS, hardware-secured modules, and encrypted communication frameworks. Moreover, the shift toward electric vehicles and connected ADAS features increases cybersecurity complexity, requiring multi-layer protection for infotainment, telematics, and autonomous driving stacks. Substantial contributions from the Asia Pacific region, especially China, combined with increasing investments from Europe and North America, are accelerating the global adoption of advanced connected car security architectures.

https://mnmimg.marketsandmarkets.com/Images/connected-car-security-market-img-overview.webp

"By form, the in-vehicle solutions segment is projected to account for a larger share than the external cloud services segment during the forecast period."
The dominance of in-vehicle security solutions is driven by the rising complexity of electronic control units (ECUs), domain controllers, and telematics systems, which require embedded protection to prevent unauthorized access and system manipulation. Compliance mandates under UNECE WP.29, ISO/SAE 21434, and China's Automotive Data Security Regulations have

accelerated OEM adoption of secure gateways, hardware security modules (HSMs), and intrusion detection systems inside the vehicle architecture. As connected ADAS, digital cockpits, and V2X communication become standard across mid-range and premium models, in-vehicle security becomes the core protection layer for safeguarding internal networks, OTA software, and data flows. This sustained regulatory and technological push positions in-vehicle solutions as the largest revenue-generating segment in the market.

?

"By solution type, the hardware-based solutions segment is projected to be a faster-growing segment than the software-based segment during the forecast period."

The use of hardware-based solutions is expanding rapidly due to the industry's shift toward tamper-resistant architectures that ensure secure data processing, cryptographic key storage, and real-time threat mitigation at the ECU level. Components such as TPMs, HSMs, secure microcontrollers, and cryptographic accelerators are becoming essential for protecting safety-critical ADAS systems, high-performance computing units, and autonomous driving platforms. With rising cybersecurity threats targeting vehicle firmware and communication buses, OEMs are increasingly adopting hardware-rooted trust models for stronger authentication and encryption. Growing SDV adoption and the need for secured zonal architectures further accelerate demand, making hardware-based solutions the fastest-growing segment despite higher integration costs.

"Asia Pacific is projected to be the fastest-growing segment in the global connected car security market during the forecast period."

Asia Pacific is projected to witness strong and accelerating growth driven by the rapid expansion of connected and autonomous mobility ecosystems in China, Japan, South Korea, and India. China is leading this momentum through the strict enforcement of the automotive data security regulations, compelling OEMs such as BYD, NIO, XPeng, Zeekr, and SAIC to adopt encrypted in-vehicle communication, secure OTA platforms, and embedded IDS/IPS solutions. Japan and South Korea are advancing deployments in line with UNECE WP.29 CSMS frameworks, supported by robust telematics networks and high connected car penetration across both luxury and mass-market segments. With rapid EV adoption, strong 5G rollout, and government-led cybersecurity compliance, Asia Pacific continues to generate significant new revenue opportunities, making it the fastest-growing region in the connected car security market.

In-depth interviews were conducted with CEOs, marketing directors, other innovation and technology directors, and executives from various key organizations operating in this market.

-□By Company Type: OEMs - 10% and Tier 1 Companies - 90%
-□By Designation: C-Level Executive - 60%; Director-Level - 30%; Others - 10%
-□By Region: North America - 40%; Europe - 50%; and Asia Pacific - 10%

Note: Others include Sales Managers and Product Managers.

The connected car security market is dominated by major players, such as NXP Semiconductors (Netherlands), AUMOVIO SE (Germany), Harman International (US), Vector Informatik GmbH (Germany), BlackBerry Limited (Canada), Thales (France), ARM Limited (UK), WirelessCar (Sweden), Astemo Ltd. (Japan), and Keysight Technologies (US. These companies are expanding their portfolios to strengthen their connected car security market position.

Research Coverage

The report covers the connected car security market in terms of security type (Endpoint Security, Application Security, Network Security, and Cloud Security), application [Telematics Control Units (TCUs), Infotainment Systems, ADAS & Autonomous Driving Systems, and Communication Modules], electric vehicle type (BEV, PHEV, HEV, and FCEV), solution type (Software-based Solutions and Hardware-based Solutions), form (In-Vehicle Solutions and External Cloud Services), and Region (North America, Asia Pacific, Europe, and Rest of the World). It covers the competitive landscape and company profiles of the key players in the significant connected car security market.

The study also includes an in-depth competitive analysis of the key market players, their company profiles, key observations related to product and business offerings, recent developments, and key market strategies.

Key Benefits of Buying the Report:

-□The report will help market leaders/new entrants with information on the closest approximations of revenue numbers for the

connected car security market and its subsegments.
-□This report will help stakeholders understand the competitive landscape and gain more insights, enabling them to position their businesses better and plan suitable go-to-market strategies.
-□The report will also help stakeholders understand the market pulse and provide information on key market drivers, restraints, challenges, and opportunities.
-□The report will also help stakeholders understand the current and future pricing trends of the connected car security market.
The report also provides insights into the following pointers:
-□Analysis of key drivers (Increasing vehicle connectivity through telematics and V2X, mandatory compliance with global automotive cybersecurity regulations, and rising cyberattacks on connected and autonomous vehicles), restraints (Legacy ECU and vehicle architectures complicate security upgrades and high implementation and integration costs), opportunities (Growth of managed security services and vehicle SOCs, rising demand for secure OTA and lifecycle management, and V2X and 5G networks requiring strong PKI-based security), and challenges (Evolving cyber threats and minimizing false positives without compromising safety-critical functions)
-□Product Developments/Innovation: Detailed insights into upcoming technologies, research & development activities, and product & service launches in the connected car security market.
-□Market Development: Comprehensive information about lucrative markets across varied regions
-□Market Diversification: Exhaustive information about new products & services, untapped geographies, recent developments, and investments in the connected car security market
-□Competitive Assessment: In-depth assessment of market share, growth strategies, and service offerings of leading players like as NXP Semiconductors (Netherlands), AUMOVIO SE (Germany), Harman International (US), Vector Informatik GmbH (Germany), BlackBerry Limited (Canada), Thales (France), ARM Limited (UK), WirelessCar (Sweden), Astemo Ltd. (Japan), and Keysight Technologies (US), among others, in connected car security market

Table of Contents:

Connected Car Security Market by Type (Endpoint, Application, Network, Security), Solution (Software & Hardware), Application (TCU, Infotainment, ADAS, Communication Modules), Form (In-vehicle, External Cloud), EV Type & Region - Global Forecast to 2032

Market Report | 2025-12-05 | 278 pages | MarketsandMarkets

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	$4950.00
	Multi User	$6650.00
	Corporate License	$8150.00
	Enterprise Site License	$10000.00
	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	2026-02-11
		Signature	