Connected Car Security Market Opportunity, Growth Drivers, Industry Trend Analysis, and Forecast 2026 - 2035

Market Report | 2026-02-13 | 260 pages | Global Market Insights

AVAILABLE LICENSES:

- Single User $4850.00
- Multi User $6050.00
- Enterprise User $8350.00

Report description:

The Global Connected Car Security Market was valued at USD 3.9 billion in 2025 and is estimated to grow at a CAGR of 13.6% to reach USD 13.8 billion by 2035.

The rapid adoption of connected car technologies has created an urgent need for robust cybersecurity across vehicle ecosystems, fleet management platforms, and cloud-connected services. Automakers and enterprises are increasingly embedding security features directly into vehicle electronic architectures, backend servers, and cloud platforms to reduce operational risks and reliance on manual monitoring. Continuous advancements in edge AI processors, V2X communications, and vehicle software platforms are enhancing the performance, scalability, and responsiveness of security solutions. Real-time intrusion detection, secure data exchange, and over-the-air updates are becoming standard to protect large vehicle fleets. Strategic alliances, mergers, and collaborations among automotive OEMs, cybersecurity providers, and cloud operators are accelerating the integration of security into the vehicle lifecycle, fleet operations, and mobility services. Connected car security is evolving from conventional monitoring to AI-powered, proactive threat analysis systems that safeguard software-defined vehicles and mobility platforms.

The In-vehicle solutions segment held 64.8% share in 2025 and is expected to grow at a CAGR of 12.1% through 2035. These solutions provide embedded security across electronic control units, domain controllers, telematics modules, and infotainment systems, enabling real-time monitoring, intrusion prevention, and secure communications. OEMs prioritize in-vehicle security to meet regulatory and safety standards while ensuring vehicle systems are resilient to cyberattacks.

The network security segment accounted for 43.8% share in 2025 and is projected to grow at a CAGR of 12.8% from 2026 to 2035. Network security safeguards vehicle communication networks, in-vehicle data buses, and cloud connections against cyber threats, providing robust protocols, real-time monitoring, and breach mitigation. It remains a critical requirement for OEMs, fleet operators, and mobility service providers to maintain system integrity.

US Connected Car Security Market generated USD 1.4 billion in 2025, and continues to grow as automakers, fleet operators, and technology firms invest in advanced cybersecurity platforms. Companies deploy integrated hardware and software solutions to protect telematics, V2X communications, and in-vehicle networks, ensuring compliance with safety and regulatory requirements

for both internal combustion and electric vehicles.
Leading players in the Global Connected Car Security Market include ARM, AUMOVIO, BlackBerry, Harman International, Intertek, Keysight Technologies, KPIT Technologies, NXP Semiconductors, Secunet Security Networks, and Thales. Companies in the Global Connected Car Security Market are strengthening their foothold by investing in AI-powered intrusion detection, over-the-air threat management, and secure vehicle software stacks. They are forming strategic partnerships with OEMs, mobility service providers, and cloud vendors to integrate security across vehicle lifecycles and connected platforms. Firms are prioritizing R&D for edge AI, V2X protection, and secure telematics modules while expanding global deployment of security solutions. Emphasis is placed on compliance with automotive cybersecurity regulations, predictive threat intelligence, and real-time network monitoring.
□
□

Table of Contents:

Report Content

Chapter 1 Methodology
1.1 Research approach
1.2 Quality commitments
1.2.1 GMI AI policy & data integrity commitment
1.3 Research trail & confidence scoring
1.3.1 Research trail components
1.3.2 Scoring components
1.4 Data collection
1.4.1 Partial list of primary sources
1.5 Data mining sources
1.5.1 Paid sources
1.6 Base estimates and calculations
1.6.1 Base year calculation
1.7 Forecast model
1.8 Research transparency addendum

Chapter 2 Executive Summary
2.1 Industry 360 synopsis
2.2 Key market trends
2.2.1 Regional
2.2.2 Security
2.2.3 Form
2.2.4 Solution
2.2.5 Vehicle
2.2.6 Propulsion
2.2.7 Application
2.3 TAM analysis, 2026-2035
2.4 CXO perspectives: Strategic imperatives
2.4.1 Executive decision points
2.4.2 Critical success factors
2.5 Future outlook
2.6 Strategic recommendations

Chapter 3 Industry Insights
3.1 Industry ecosystem analysis
3.1.1 Supplier landscape
3.1.2 Profit margin
3.1.3 Cost structure
3.1.4 Value addition at each stage
3.1.5 Factor affecting the value chain
3.1.6 Disruptions
3.2 Industry impact forces
3.2.1 Growth drivers
3.2.1.1 Rising adoption of connected and software-defined vehicles
3.2.1.2 Increasing cybersecurity threats targeting automotive systems
3.2.1.3 Regulatory mandates and safety standards
3.2.1.4 Growth of electric, autonomous, and shared mobility vehicles
3.2.2 Industry pitfalls and challenges
3.2.2.1 Complexity of securing heterogeneous vehicle architectures
3.2.2.2 Data privacy and cross-border regulatory compliance issues
3.2.3 Market opportunities
3.2.3.1 Integration of security into vehicle software platforms and OTA ecosystems
3.2.3.2 Expansion of V2X, 5G, and cloud-based vehicle services
3.2.3.3 Rising adoption of hardware-based security solutions
3.2.3.4 Growing focus on autonomous driving and ADAS security
3.3 Growth potential analysis
3.4 Regulatory landscape
3.4.1 North America
3.4.1.1 National Highway Traffic Safety Administration (NHTSA)
3.4.1.2 U.S. Department of Commerce / Bureau of Industry and Security (BIS)
3.4.1.3 Federal Trade Commission (FTC)
3.4.2 Europe
3.4.2.1 UNECE WP.29 Regulations (UN R155 & R156)
3.4.2.2 EN / ISO Automotive Standards
3.4.3 Asia Pacific
3.4.3.1 China National Standards for Vehicle Cybersecurity
3.4.3.2 India Automotive Standards (AIS 189 & AIS 190)
3.4.4 Latin America
3.4.4.1 Brazil: LGPD (Lei Geral de Protecao de Dados)
3.4.4.2 Mexico: NOM Standards
3.4.5 Middle East & Africa
3.4.5.1 UAE & Gulf States: IoT & V2X Security Policy
3.4.5.2 Saudi Arabia: SDAIA Automotive AI Framework
3.4.5.3 African Union (AU): Data Policy Framework
3.5 Porter's analysis
3.6 PESTEL analysis
3.7 Technology and innovation landscape
3.7.1 Current technological trends
3.7.2 Emerging technologies

3.8 Pricing trend analysis
3.9 Patent analysis
3.10 Sustainability and environmental aspects
3.10.1 Sustainable practices
3.10.2 Energy efficiency in production
3.10.3 Carbon footprint considerations
3.11 Data Governance, Cybersecurity, and Model Risk
3.11.1 Data Privacy and Compliance
3.11.2 Model Security
3.11.3 Operational and Systemic Risks
3.12 Security Architecture
3.12.1 Multi-layer Security Models
3.12.2 Vehicle-to-Everything (V2X) Security

Chapter 4 Competitive Landscape, 2025
4.1 Introduction
4.2 Company market share analysis
4.2.1 North America
4.2.2 Europe
4.2.3 Asia Pacific
4.2.4 LATAM
4.2.5 MEA
4.3 Competitive analysis of major market players
4.4 Competitive positioning matrix
4.5 Strategic outlook matrix
4.6 Key developments
4.6.1 Mergers & acquisitions
4.6.2 Partnerships & collaborations
4.6.3 New product launches
4.6.4 Expansion plans and funding

Chapter 5 Market Estimates & Forecast, By Security, 2022 - 2035 ($Mn)
5.1 Key trends
5.2 Endpoint security
5.3 Application security
5.4 Network security
5.5 Cloud security

Chapter 6 Market Estimates & Forecast, By Form, 2022 - 2035 ($Mn)
6.1 Key trends
6.2 In-Vehicle Solutions
6.3 External Cloud Services

Chapter 7 Market Estimates & Forecast, By Solution, 2022 - 2035 ($Mn)
7.1 Key trends
7.2 Software
7.3 Hardware

7.3.1 Hardware security modules (HSM)
7.3.2 Secure microcontrollers
7.3.3 Trusted platform modules (TPM)
7.3.4 Secure gateways
7.3.5 Others

Chapter 8 Market Estimates & Forecast, By Vehicle, 2022 - 2035 ($Mn)
8.1 Key trends
8.2 Hatchback
8.3 Sedan
8.4 SUV

Chapter 9 Market Estimates & Forecast, By Propulsion, 2022 - 2035 ($Mn)
9.1 Key trends
9.2 Internal combustion engine (ICE)
9.3 Electric vehicle
9.3.1 Battery electric vehicle (BEV)
9.3.2 Plug-in hybrid electric vehicle (PHEV)
9.3.3 Hybrid electric vehicle (HEV)
9.3.4 Fuel cell electric vehicle (FCEV)

Chapter 10 Market Estimates & Forecast, By Application, 2022 - 2035 ($Mn)
10.1 Key trends
10.2 Telematics control units (TCUS)
10.3 Infotainment systems
10.4 Adas & autonomous driving systems
10.5 Communication modules
10.6 Others

Chapter 11 Market Estimates & Forecast, By Region, 2022 - 2035 ($Mn)
11.1 Key trends
11.2 North America
11.2.1 US
11.2.2 Canada
11.3 Europe
11.3.1 Germany
11.3.2 UK
11.3.3 France
11.3.4 Italy
11.3.5 Spain
11.3.6 Nordics
11.3.7 Russia
11.3.8 Norway
11.3.9 Denmark
11.3.10 Netherlands
11.3.11 Belgium
11.4 Asia Pacific

11.4.1 China
11.4.2 India
11.4.3 Japan
11.4.4 South Korea
11.4.5 ANZ
11.4.6 Vietnam
11.4.7 Indonesia
11.4.8 Singapore
11.4.9 Malaysia
11.4.10 Thailand
11.5 Latin America
11.5.1 Brazil
11.5.2 Mexico
11.5.3 Argentina
11.6 MEA
11.6.1 South Africa
11.6.2 Saudi Arabia
11.6.3 UAE

Chapter 12 Company Profiles
12.1 Global companies
12.1.1 BlackBerry
12.1.2 NXP Semiconductors
12.1.3 Harman International
12.1.4 Thales
12.1.5 ARM
12.1.6 Trend Micro
12.1.7 Keysight Technologies
12.1.8 Intertek
12.1.9 T-Systems International
12.1.10 KPIT Technologies
12.1.11 Tata Elxsi
12.2 Regional players
12.2.1 AUMOVIO
12.2.2 Vector Informatik
12.2.3 ETAS
12.2.4 ASTEMO
12.2.5 Autocrypt
12.2.6 Secunet Security Networks
12.2.7 Trustonic
12.2.8 Device Authority
12.2.9 WirelessCar
12.3 Emerging players
12.3.1 Upstream Security
12.3.2 Trillium Secure
12.3.3 Karamba Security
12.3.4 Intertrust Technologies

12.3.5 GuardKnox

Connected Car Security Market Opportunity, Growth Drivers, Industry Trend Analysis, and Forecast 2026 - 2035

Market Report | 2026-02-13 | 260 pages | Global Market Insights

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	$4850.00
	Multi User	$6050.00
	Enterprise User	$8350.00
	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	2026-03-30
		Signature