+357 96 030922
info@marketpublishers.com

Connected Car Cybersecurity Market Forecasts to 2032 – Global Analysis By Security Type (Endpoint Security, Wireless Communication Security, Application Security, Cloud Security, and Network Security), Solution, Vehicle Connectivity, Vehicle Type, Application and By Geography

https://marketpublishers.com/r/C4A02CF505C0EN.html
Date: October 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: C4A02CF505C0EN

Abstracts

According to Stratistics MRC, the Global Connected Car Cybersecurity Market is accounted for $2.4 billion in 2025 and is expected to reach $8.1 billion by 2032 growing at a CAGR of 18.5% during the forecast period. Connected Car Cybersecurity refers to the protection of digital systems and data within vehicles that are connected to external networks. It involves safeguarding communication channels, embedded software, sensors, and cloud-based services from unauthorized access or cyberattacks. The focus is on ensuring data privacy, secure connectivity, and system integrity in vehicle-to-everything (V2X) communications. Solutions include encryption, intrusion detection, secure gateways, and firmware protection to maintain safety and prevent manipulation of critical automotive functions.

According to Gartner, rising automotive data vulnerabilities and increasing connected vehicle adoption have accelerated demand for endpoint and hardware security solutions, with global investment in vehicle cybersecurity projected to grow over 20% annually.

Market Dynamics:

Driver:

+357 96 030922
info@marketpublishers.com

Increasing automotive data vulnerability

Increasing automotive data vulnerability has become a primary growth catalyst for the Connected Car Cybersecurity Market. As vehicles integrate advanced connectivity and telematics systems, the volume of transmitted data between vehicles and external networks has surged. This has heightened the risk of data breaches, malware infiltration, and unauthorized access to vehicle systems. Consequently, automakers and cybersecurity providers are increasingly prioritizing robust protection frameworks. The growing awareness of data protection compliance further strengthens market demand across the automotive cybersecurity landscape.

Restraint:

Lack of global cybersecurity standards

The lack of global cybersecurity standards significantly restrains the Connected Car Cybersecurity Market's expansion. Automotive manufacturers face challenges in aligning with fragmented regulatory frameworks across regions, leading to inconsistent implementation of security measures. The absence of a unified protocol complicates interoperability between hardware, software, and communication networks. This variability often results in longer validation cycles and increased compliance costs. Moreover, it discourages smaller automotive suppliers from adopting comprehensive cybersecurity frameworks, impeding seamless ecosystem integration.

Opportunity:

Partnerships with OEMs for security

Partnerships with Original Equipment Manufacturers (OEMs) for security integration present substantial opportunities for market participants. These collaborations enable cybersecurity firms to embed protection mechanisms directly into vehicle architecture during early development stages. Such partnerships enhance system resilience against cyberattacks and create long-term service contracts. Additionally, OEM alliances foster innovation through joint research and regulatory compliance alignment. This co-development model ensures robust data protection frameworks and helps manufacturers differentiate vehicles through enhanced digital safety features.

Threat:

+357 96 030922
info@marketpublishers.com

Limited skilled cybersecurity workforce

A limited skilled cybersecurity workforce poses a major threat to the market's scalability. The rising complexity of connected vehicle systems demands specialized expertise in threat detection, encryption, and AI-driven defense mechanisms. However, the global talent shortage restricts timely system audits and vulnerability assessments. As a result, automakers struggle to maintain proactive cyber protection. The scarcity of skilled professionals may delay technology rollouts, increasing exposure to attacks and weakening industry confidence in connected mobility solutions.

Covid-19 Impact:

The COVID-19 pandemic initially slowed vehicle production and cybersecurity implementation due to supply chain disruptions and budget constraints. However, it accelerated digital transformation across the automotive ecosystem, emphasizing the importance of remote connectivity and over-the-air updates. This shift underscored vulnerabilities in digital vehicle platforms, prompting manufacturers to strengthen security architectures. Increased reliance on connected technologies during lockdowns further expanded the market's long-term relevance. Consequently, cybersecurity investments became integral to post-pandemic automotive innovation strategies.

The endpoint security segment is expected to be the largest during the forecast period

The endpoint security segment is expected to account for the largest market share during the forecast period, owing to its crucial role in safeguarding communication interfaces such as infotainment systems, telematics units, and onboard control modules. As vehicles become increasingly software-defined, endpoint protection ensures real-time monitoring and encryption of critical data. Furthermore, rising adoption of connected platforms and frequent OTA updates elevate the need for advanced endpoint defense mechanisms within modern automotive architectures.

The hardware security modules (HSM) segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the hardware security modules (HSM) segment is predicted to witness the highest growth rate, reinforced by their ability to securely manage cryptographic keys and authentication processes. HSMs enhance tamper resistance, protect vehicle-to-cloud communication, and support secure boot functions. With rising vehicle connectivity and autonomous capabilities, demand for embedded HSMs has

+357 96 030922
info@marketpublishers.com

surged. Manufacturers increasingly integrate these components to meet compliance standards and prevent unauthorized system manipulation across connected automotive platforms.

Region with largest share:

During the forecast period, the Asia Pacific region is expected to hold the largest market share, ascribed to rapid vehicle digitization and growing adoption of connected car technologies in countries like China, Japan, and South Korea. Regional automakers are investing heavily in in-vehicle security solutions to address government regulations on data protection and vehicle communication. Moreover, the presence of leading electronics manufacturers accelerates innovation in automotive cybersecurity hardware and software, further strengthening regional dominance.

Region with highest CAGR:

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR associated with robust adoption of advanced driver-assistance systems (ADAS) and autonomous driving platforms. Stringent cybersecurity regulations by agencies such as NHTSA and DOT have pushed automakers toward enhanced digital defense frameworks. Additionally, strong collaboration between automakers and cybersecurity firms in the U.S. and Canada fosters rapid innovation. Increasing investments in cloud-based automotive infrastructure continue to accelerate North America’s growth trajectory.

Key players in the market

Some of the key players in Connected Car Cybersecurity Market include Continental AG, Aptiv PLC, NXP Semiconductors N.V., Infineon Technologies AG, Qualcomm Incorporated, STMicroelectronics N.V., Texas Instruments Incorporated, NVIDIA Corporation, Analog Devices, Inc., Microchip Technology Inc., Renesas Electronics Corporation, BlackBerry Limited, Cisco Systems, Inc., Palo Alto Networks, Inc., Fortinet, Inc., Check Point Software Technologies Ltd., Trend Micro Incorporated and Broadcom Inc.

Key Developments:

In August 2025, BlackBerry Limited launched its new 'CylanceGUARD for Vehicles' service, an AI-powered threat detection and response platform. It provides real-time

+357 96 030922
info@marketpublishers.com

monitoring of in-vehicle networks to identify and neutralize sophisticated cyber-attacks targeting electronic control units (ECUs).

In July 2025, NXP Semiconductors N.V. introduced the new 'S32G3 Security Gateway Chipset,' a hardware-based solution designed for high-speed, secure vehicle-to-cloud (V2C) communication. The chipset features integrated hardware security modules (HSMs) to protect data integrity and prevent unauthorized access.

In June 2025, Continental AG announced the launch of its 'Secure Vehicle Stack' platform developed in partnership with Indian OEMs. The system provides a comprehensive, cost-effective cybersecurity solution tailored for the Indian market, ensuring compliance with upcoming regional data privacy and vehicle security regulations.

Security Types Covered:

- Endpoint Security
- Wireless Communication Security
- Application Security
- Cloud Security
- Network Security

Solutions Covered:

- Hardware Security Modules (HSM)
- Encryption and Firewalls
- Intrusion Detection & Prevention Systems (IDPS)
- Risk & Compliance Management
- Identity & Access Management (IAM)

+357 96 030922
info@marketpublishers.com

Security Information & Event Management (SIEM)

Vehicle Connectivities Covered:

Vehicle-To-Vehicle (V2V)

Vehicle-To-Infrastructure (V2I)

Vehicle-To-Cloud (V2C)

Vehicle-To-Everything (V2X)

Vehicle Types Covered:

Passenger Cars

Light Commercial Vehicles (LCVs)

Heavy Commercial Vehicles (HCVs)

Electric & Hybrid Vehicles

Applications Covered:

Telematics Systems

Infotainment Systems

ADAS & Safety Systems

Powertrain Control

Remote Diagnostics

Regions Covered:

+357 96 030922
info@marketpublishers.com

North America

US

Canada

Mexico

Europe

Germany

UK

Italy

France

Spain

Rest of Europe

Asia Pacific

Japan

China

India

Australia

New Zealand

South Korea

Rest of Asia Pacific

South America

+357 96 030922
info@marketpublishers.com

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

What our report offers:
- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- 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:

+357 96 030922
info@marketpublishers.com

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

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

10 GLOBAL CONNECTED CAR CYBERSECURITY MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

11 KEY DEVELOPMENTS

12 COMPANY PROFILING

+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 Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Connected Car Cybersecurity Market Forecasts to 2032 – Global Analysis By Security Type (Endpoint Security, Wireless Communication Security, Application Security, Cloud Security, and Network Security), Solution, Vehicle Connectivity, Vehicle Type, Application and By Geography

Product link: https://marketpublishers.com/r/C4A02CF505C0EN.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/C4A02CF505C0EN.html