

Connected Vehicle Cybersecurity Market Forecasts to 2034 – Global Analysis By Offering (Hardware, Software and Services), Vehicle Type, Application and By Geography

<https://marketpublishers.com/r/CD34F506B778EN.html>

Date: September 2026

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: CD34F506B778EN

Abstracts

According to Statistics MRC, the Global Connected Vehicle Cybersecurity Market is accounted for \$3.1 billion in 2026 and is expected to reach \$10.5 billion by 2034 growing at a CAGR of 16.4% during the forecast period. Connected vehicle cybersecurity refers to the hardware, software, and services designed to protect modern vehicles from unauthorized access, data breaches, and malicious cyberattacks. As vehicles become increasingly connected via V2X communication and equipped with advanced infotainment and autonomous driving systems, robust cybersecurity measures are critical to ensure passenger safety, data privacy, and operational integrity. The technology encompasses endpoint protection, intrusion detection, secure gateways, and managed security services tailored for passenger cars, commercial vehicles, EVs, and autonomous platforms.

Market Dynamics:

Driver:

Proliferation of connected and autonomous vehicle features

The rapid integration of advanced connectivity features, over-the-air software updates, and autonomous driving capabilities is exponentially expanding the cyberattack surface of modern vehicles. Automotive OEMs are heavily investing in comprehensive cybersecurity architectures to protect critical vehicle networks from increasingly sophisticated threats. Growing consumer expectations for seamless digital experiences within vehicles are accelerating connected feature deployment and mandatory

cybersecurity solution integration.

Restraint:

Complexity of securing legacy vehicle architectures

Integrating advanced cybersecurity protocols into legacy vehicle electronic architectures and fragmented electronic control unit ecosystems presents a formidable technical challenge. Older vehicle platforms were designed without security-by-design principles, featuring unencrypted internal communication buses that resist straightforward retrofitting. The complexity of validating security patches across heterogeneous supplier components significantly increases development costs and extends deployment timelines.

Opportunity:

Stringent global vehicle cybersecurity regulations

The implementation of stringent global regulatory frameworks, including UNECE WP.29 and ISO/SAE 21434 standards, is mandating comprehensive security lifecycle management for all new vehicle type approvals. These regulatory mandates are creating substantial market opportunities for cybersecurity providers offering compliance consulting, penetration testing, and certification support. Automakers facing strict regulatory deadlines are accelerating procurement of end-to-end cybersecurity solutions.

Threat:

Evolving sophistication of automotive cyber attacks

The continuous evolution of cyber threats targeting connected vehicles, including remote hijacking exploits and ransomware attacks on fleet management systems, poses a severe threat. Cybercriminal organizations are developing increasingly sophisticated attack tools specifically designed to exploit vehicle communication protocols. The expanding automotive software supply chain creates numerous potential entry points requiring constant, costly monitoring and rapid patch deployment capabilities.

Covid-19 Impact:

The pandemic accelerated the digitalization of the automotive industry as consumer demand surged for contactless vehicle features, remote diagnostics, and over-the-air software updates. This rapid digital transformation significantly expanded the vehicle

cyberattack surface, prompting manufacturers to substantially increase cybersecurity investment priorities. Post-pandemic supply chain disruptions also highlighted vulnerabilities in third-party software component sourcing, driving increased demand for comprehensive supply chain security auditing.

The software segment is expected to be the largest during the forecast period

The software segment is expected to account for the largest market share during the forecast period, as endpoint protection, intrusion detection systems, and secure over-the-air update managers form the primary defensive layer within connected vehicles. Continuous software updates addressing newly discovered vulnerabilities and advanced machine learning-based threat detection generate substantial recurring revenue streams. The strategic shift toward software-defined vehicle architectures is significantly amplifying the market dominance of cybersecurity software.

The autonomous vehicles segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the autonomous vehicles segment is predicted to witness the highest growth rate, driven by the critical need to protect massive volumes of real-time sensor data and AI processing pipelines. Any successful cyber compromise of an autonomous vehicle's perception or control systems could result in catastrophic safety failures. Regulatory authorities worldwide are mandating the highest cybersecurity assurance levels for autonomous certification, compelling manufacturers to invest heavily in fail-safe security designs.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, due to strong regulatory frameworks promoting vehicle safety, high corporate sustainability commitments, and the presence of leading automotive OEMs. The United States leads with significant investments in connected vehicle infrastructure and advanced cybersecurity research. Favorable government incentives for autonomous vehicle development and strong consumer demand drive market development.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, driven by rapid industrialization, massive connected vehicle production, and strong government initiatives promoting green mobility. China and India represent major growth markets with expanding cybersecurity capacities and rising demand for sustainable transit solutions. Local manufacturers are investing heavily in R&D to develop cost-effective connected vehicle cybersecurity solutions.

Key players in the market

Some of the key players in Global Connected Vehicle Cybersecurity Market include Argus Cyber Security, Upstream Security, GuardKnox Cyber Technologies, Harman International, Vector Informatik, ESCRYPT (ETAS), Thales Group, Aptiv PLC, Denso Corporation, Robert Bosch GmbH, BlackBerry Limited, Karamba Security, Cymotive (Continental), Ansys, Synopsys, Keysight Technologies, Infineon Technologies, and NXP Semiconductors.

Key Developments:

In June 2026, Upstream Security launched an advanced cloud-based automotive cybersecurity platform providing real-time threat intelligence and fleet-wide anomaly detection for connected commercial vehicles.

In May 2026, Harman International introduced a new hardware-based secure gateway module designed to protect in-vehicle infotainment systems and V2X communication channels from unauthorized access.

In April 2026, Argus Cyber Security partnered with a major European automaker to integrate its AI-driven intrusion detection system into the next-generation architecture of premium passenger cars.

Offerings Covered:

Hardware

Software

Services

Vehicle Types Covered:

Passenger Cars

Commercial Vehicles

Electric Vehicles

Autonomous Vehicles

Applications Covered:

V2X Communication Security

Infotainment Security

Powertrain Security

Advanced Driver Assistance Systems (ADAS) Security

Fleet Management Security

Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

Switzerland

Poland

Rest of Europe

Asia Pacific

China

Japan

India

South Korea

Australia

Indonesia

Thailand

Malaysia

Singapore

Vietnam

Rest of Asia Pacific

South America

Brazil

Argentina

Colombia

Chile

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of 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 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034

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:

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

Contents

1 EXECUTIVE SUMMARY

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

2 RESEARCH FRAMEWORK

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
 - 2.4.1 Data Collection (Primary and Secondary)
 - 2.4.2 Data Modeling and Estimation Techniques
 - 2.4.3 Data Validation and Triangulation
 - 2.4.4 Analytical and Forecasting Approach

3 MARKET DYNAMICS AND TREND ANALYSIS

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

4 COMPETITIVE AND STRATEGIC ASSESSMENT

- 4.1 Porter's Five Forces Analysis
 - 4.1.1 Supplier Bargaining Power
 - 4.1.2 Buyer Bargaining Power
 - 4.1.3 Threat of Substitutes
 - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

5 GLOBAL CONNECTED VEHICLE CYBERSECURITY MARKET, BY OFFERING

- 5.1 Hardware
- 5.2 Software
 - 5.2.1 Endpoint Security Software
 - 5.2.2 Intrusion Detection and Prevention Software
- 5.3 Services
 - 5.3.1 Managed Security Services
 - 5.3.2 Security Consulting Services

6 GLOBAL CONNECTED VEHICLE CYBERSECURITY MARKET, BY VEHICLE TYPE

- 6.1 Passenger Cars
 - 6.1.1 Connected Passenger Cars
 - 6.1.2 Premium Passenger Cars
- 6.2 Commercial Vehicles
- 6.3 Electric Vehicles
 - 6.3.1 Battery Electric Vehicles (BEVs)
 - 6.3.2 Plug-in Hybrid Electric Vehicles (PHEVs)
- 6.4 Autonomous Vehicles

7 GLOBAL CONNECTED VEHICLE CYBERSECURITY MARKET, BY APPLICATION

- 7.1 V2X Communication Security
- 7.2 Infotainment Security
 - 7.2.1 In-Vehicle Infotainment Security
 - 7.2.2 Smartphone and Device Connectivity Security
 - 7.2.3 Multimedia and Application Security
- 7.3 Powertrain Security
- 7.4 Advanced Driver Assistance Systems (ADAS) Security
- 7.5 Fleet Management Security

8 GLOBAL CONNECTED VEHICLE CYBERSECURITY MARKET, BY GEOGRAPHY

- 8.1 North America
 - 8.1.1 United States
 - 8.1.2 Canada
 - 8.1.3 Mexico
- 8.2 Europe
 - 8.2.1 United Kingdom
 - 8.2.2 Germany
 - 8.2.3 France
 - 8.2.4 Italy
 - 8.2.5 Spain
 - 8.2.6 Netherlands
 - 8.2.7 Belgium
 - 8.2.8 Sweden
 - 8.2.9 Switzerland
 - 8.2.10 Poland
 - 8.2.11 Rest of Europe
- 8.3 Asia Pacific
 - 8.3.1 China
 - 8.3.2 Japan
 - 8.3.3 India
 - 8.3.4 South Korea
 - 8.3.5 Australia
 - 8.3.6 Indonesia
 - 8.3.7 Thailand
 - 8.3.8 Malaysia
 - 8.3.9 Singapore
 - 8.3.10 Vietnam
 - 8.3.11 Rest of Asia Pacific
- 8.4 South America
 - 8.4.1 Brazil
 - 8.4.2 Argentina
 - 8.4.3 Colombia
 - 8.4.4 Chile
 - 8.4.5 Peru
 - 8.4.6 Rest of South America
- 8.5 Rest of the World (RoW)
 - 8.5.1 Middle East
 - 8.5.1.1 Saudi Arabia
 - 8.5.1.2 United Arab Emirates

- 8.5.1.3 Qatar
- 8.5.1.4 Israel
- 8.5.1.5 Rest of Middle East
- 8.5.2 Africa
 - 8.5.2.1 South Africa
 - 8.5.2.2 Egypt
 - 8.5.2.3 Morocco
 - 8.5.2.4 Rest of Africa

9 STRATEGIC MARKET INTELLIGENCE

- 9.1 Industry Value Network and Supply Chain Assessment
- 9.2 White-Space and Opportunity Mapping
- 9.3 Product Evolution and Market Life Cycle Analysis
- 9.4 Channel, Distributor, and Go-to-Market Assessment

10 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

- 10.1 Mergers and Acquisitions
- 10.2 Partnerships, Alliances, and Joint Ventures
- 10.3 New Product Launches and Certifications
- 10.4 Capacity Expansion and Investments
- 10.5 Other Strategic Initiatives

11 COMPANY PROFILES

- 11.1 Argus Cyber Security
- 11.2 Upstream Security
- 11.3 GuardKnox Cyber Technologies
- 11.4 Harman International
- 11.5 Vector Informatik
- 11.6 ESCRYPT (ETAS)
- 11.7 Thales Group
- 11.8 Aptiv PLC
- 11.9 Denso Corporation
- 11.10 Robert Bosch GmbH
- 11.11 BlackBerry Limited
- 11.12 Karamba Security
- 11.13 Cymotive (Continental)

11.14 Ansys

11.15 Synopsys

11.16 Keysight Technologies

11.17 Infineon Technologies

11.18 NXP Semiconductors

List of Tables

Table 1 Global Connected Vehicle Cybersecurity Market Outlook, By Region
(2023-2034) (\$MN)

Table 2 Global Connected Vehicle Cybersecurity Market Outlook, By Offering
(2023-2034) (\$MN)

Table 3 Global Connected Vehicle Cybersecurity Market Outlook, By Hardware
(2023-2034) (\$MN)

Table 4 Global Connected Vehicle Cybersecurity Market Outlook, By Software
(2023-2034) (\$MN)

Table 5 Global Connected Vehicle Cybersecurity Market Outlook, By Endpoint Security
Software (2023-2034) (\$MN)

Table 6 Global Connected Vehicle Cybersecurity Market Outlook, By Intrusion Detection
and Prevention Software (2023-2034) (\$MN)

Table 7 Global Connected Vehicle Cybersecurity Market Outlook, By Services
(2023-2034) (\$MN)

Table 8 Global Connected Vehicle Cybersecurity Market Outlook, By Managed Security
Services (2023-2034) (\$MN)

Table 9 Global Connected Vehicle Cybersecurity Market Outlook, By Security
Consulting Services (2023-2034) (\$MN)

Table 10 Global Connected Vehicle Cybersecurity Market Outlook, By Vehicle Type
(2023-2034) (\$MN)

Table 11 Global Connected Vehicle Cybersecurity Market Outlook, By Passenger Cars
(2023-2034) (\$MN)

Table 12 Global Connected Vehicle Cybersecurity Market Outlook, By Connected
Passenger Cars (2023-2034) (\$MN)

Table 13 Global Connected Vehicle Cybersecurity Market Outlook, By Premium
Passenger Cars (2023-2034) (\$MN)

Table 14 Global Connected Vehicle Cybersecurity Market Outlook, By Commercial
Vehicles (2023-2034) (\$MN)

Table 15 Global Connected Vehicle Cybersecurity Market Outlook, By Electric Vehicles
(2023-2034) (\$MN)

Table 16 Global Connected Vehicle Cybersecurity Market Outlook, By Battery Electric
Vehicles (BEVs) (2023-2034) (\$MN)

Table 17 Global Connected Vehicle Cybersecurity Market Outlook, By Plug-in Hybrid

Electric Vehicles (PHEVs) (2023-2034) (\$MN)

Table 18 Global Connected Vehicle Cybersecurity Market Outlook, By Autonomous Vehicles (2023-2034) (\$MN)

Table 19 Global Connected Vehicle Cybersecurity Market Outlook, By Application (2023-2034) (\$MN)

Table 20 Global Connected Vehicle Cybersecurity Market Outlook, By V2X Communication Security (2023-2034) (\$MN)

Table 21 Global Connected Vehicle Cybersecurity Market Outlook, By Infotainment Security (2023-2034) (\$MN)

Table 22 Global Connected Vehicle Cybersecurity Market Outlook, By In-Vehicle Infotainment Security (2023-2034) (\$MN)

Table 23 Global Connected Vehicle Cybersecurity Market Outlook, By Smartphone and Device Connectivity Security (2023-2034) (\$MN)

Table 24 Global Connected Vehicle Cybersecurity Market Outlook, By Multimedia and Application Security (2023-2034) (\$MN)

Table 25 Global Connected Vehicle Cybersecurity Market Outlook, By Powertrain Security (2023-2034) (\$MN)

Table 26 Global Connected Vehicle Cybersecurity Market Outlook, By Advanced Driver Assistance Systems (ADAS) Security (2023-2034) (\$MN)

Table 27 Global Connected Vehicle Cybersecurity Market Outlook, By Fleet Management Security (2023-2034) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) Regions are also represented in the same manner as above.

I would like to order

Product name: Connected Vehicle Cybersecurity Market Forecasts to 2034 – Global Analysis By Offering (Hardware, Software and Services), Vehicle Type, Application and By Geography

Product link: <https://marketpublishers.com/r/CD34F506B778EN.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/CD34F506B778EN.html>