+357 96 030922
info@marketpublishers.com

# Vehicle Cybersecurity Market Forecasts to 2032 – Global Analysis By Security Type (Network Security, Application Security, Cloud Security, Endpoint Security, and Wireless Security), Propulsion Type, Vehicle Type, Application, End User, and By Geography.

https://marketpublishers.com/r/V0EE4A82165FEN.html
Date: April 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: V0EE4A82165FEN

## Abstracts

According to Stratistics MRC, the Global Vehicle Cybersecurity Market is accounted for $1.1 billion in 2025 and is expected to reach $2.7 billion by 2032 growing at a CAGR of 14.1% during the forecast period. Vehicle Cybersecurity refers to the protection of digital systems within a vehicle from unauthorized access, manipulation, or damage. Modern vehicles contain software that controls navigation, communication, entertainment, and safety features. Cybersecurity measures include encryption, firewalls, intrusion detection, and secure coding practices to safeguard these systems. The goal is to prevent hacking, data theft, and system failures that could compromise safety or privacy. It ensures that vehicles operate reliably and securely in connected environments.

According to Upstream Security, modern vehicles process over 25 GB of data hourly, creating multiple attack surfaces that require specialized cybersecurity solutions to protect critical systems like brakes and steering from hackers.

**Market Dynamics:**

Driver:

Connected and autonomous vehicle expansion

+357 96 030922
info@marketpublishers.com

The Vehicle Cybersecurity Market is being driven by the rapid proliferation of connected and autonomous vehicles, which increasingly rely on software and networked systems for navigation, infotainment, and safety. Fueled by growing IoT integration, these vehicles are vulnerable to cyberattacks, prompting automakers to invest in robust security solutions. Additionally, consumer demand for safe, reliable, and data-secure vehicles is accelerating adoption. As connected mobility expands globally, the need for proactive cybersecurity frameworks becomes a critical market driver.

Restraint:

Cost of comprehensive solutions

High costs associated with implementing comprehensive vehicle cybersecurity solutions remain a significant market restraint. Advanced encryption, intrusion detection systems, and real-time monitoring require substantial investment, especially for small and mid-sized automakers. Additionally, integrating these solutions into legacy systems can further escalate expenses. Cost pressures may delay adoption in emerging markets and limit deployment across vehicle fleets. Consequently, financial constraints pose a challenge to the widespread implementation of end-to-end cybersecurity measures in the automotive sector.

Opportunity:

Partnerships with tech firms

Collaborations between automakers and technology firms present substantial growth opportunities for the Vehicle Cybersecurity Market. Partnerships enable access to cutting-edge AI, machine learning, and blockchain solutions that enhance threat detection and mitigation. Tech collaborations also facilitate faster development of over-the-air security updates and predictive risk analytics. Additionally, joint initiatives improve compliance with evolving regulatory standards and cybersecurity certifications. Such strategic alliances position stakeholders to deliver secure, scalable, and future-ready mobility solutions, expanding market potential.

Threat:

Rapidly evolving threats

+357 96 030922
info@marketpublishers.com

The Vehicle Cybersecurity Market faces threats from rapidly evolving cyberattack techniques, including ransomware, malware, and vehicle-to-everything (V2X) vulnerabilities. Hackers continuously exploit software flaws in connected and autonomous vehicles, increasing risk exposure for OEMs and consumers. The dynamic threat landscape requires continuous system updates and advanced monitoring, raising operational complexity. Furthermore, regulatory and liability concerns amplify the stakes for automakers. Failure to adapt quickly can lead to financial loss, reputational damage, and reduced consumer trust, constraining market growth.

**Covid-19 Impact:**

The COVID-19 pandemic temporarily disrupted vehicle production and supply chains but simultaneously accelerated digitalization and connected mobility adoption. With increased reliance on telematics, remote diagnostics, and over-the-air updates, the demand for robust cybersecurity solutions intensified. Automakers and fleet operators prioritized protecting data integrity and system resilience. Additionally, remote work and software-focused R&D initiatives advanced security innovation. Overall, COVID-19 highlighted vulnerabilities in vehicle networks and reinforced the importance of cybersecurity as a critical investment for the automotive industry.

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

The network security segment is expected to account for the largest market share during the forecast period, resulting from its crucial role in safeguarding vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Network security solutions protect against unauthorized access, data breaches, and service disruptions in connected and autonomous vehicles. Increasing deployment of telematics, infotainment systems, and cloud-connected platforms further drives adoption. Additionally, regulatory emphasis on cybersecurity compliance strengthens the segment’s dominance in the market.

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

Over the forecast period, the electric vehicles segment is predicted to witness the highest growth rate, propelled by the rapid expansion of EV adoption and associated connectivity features. EVs rely heavily on software-driven battery management, charging networks, and telematics, increasing vulnerability to cyber threats. Consequently, automakers are prioritizing cybersecurity integration in EV designs.

+357 96 030922
info@marketpublishers.com

Rising government incentives for EV production and growing consumer demand for secure, sustainable mobility amplify the segment's growth trajectory.

**Region with largest share:**

During the forecast period, the Asia Pacific region is expected to hold the largest market share, attributed to the region's expanding automotive production, high adoption of connected vehicles, and supportive government policies. China, Japan, and South Korea are leading the integration of autonomous and smart vehicle technologies. Additionally, increasing investment by OEMs and cybersecurity solution providers strengthens regional capabilities. Growing consumer awareness regarding vehicle safety and data privacy further consolidates Asia Pacific's dominance in the vehicle cybersecurity market.

**Region with highest CAGR:**

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR associated with advanced automotive technologies, high EV penetration, and early adoption of connected and autonomous vehicles. The U.S. market benefits from robust R&D infrastructure, strategic partnerships between tech and automotive firms, and stringent cybersecurity regulations. Rising fleet electrification and mobility services adoption further drive demand. Continuous innovation in threat detection, encryption, and over-the-air updates positions North America as the fastest-growing regional market for vehicle cybersecurity.

**Key players in the market**

Some of the key players in Vehicle Cybersecurity Market include Bosch Mobility Solutions, Continental AG, Harman International, Aptiv PLC, DENSO, BlackBerry, Intertek, Karamba Security, Lear Corporation, NXP Semiconductors, Upstream Security, Capgemini, Argus Cyber Security, Cybellum, ETAS, Infineon Technologies AG, and Panasonic Holdings.

**Key Developments:**

In August 2025, Harman International introduced its "Shield-X" platform for over-the-air threat response and ECU hardening. The system integrates with OEM cloud and supports predictive security analytics.

+357 96 030922
info@marketpublishers.com

In August 2025, Cybellum launched its “Cyber Digital Twin” platform for continuous vulnerability management. The system maps software BOMs and supports compliance with ISO 21434 and WP.29.

In February 2025, Infineon Technologies launched its AURIX™ TC4x family with enhanced HSM and post-quantum cryptography support. The chips target secure automotive architectures and V2X applications.

Security Types Covered:

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

Propulsion Types Covered:

- Internal Combustion Engine (ICE) Vehicles
- Electric Vehicles

Vehicle Types Covered:

- Passenger Cars
- Light Commercial Vehicles
- Heavy Commercial Vehicles
- Electric Vehicles

+357 96 030922
info@marketpublishers.com

Applications Covered:

- Telematics Systems
- Infotainment Systems
- Powertrain Systems
- Body Control & Comfort Systems
- ADAS & Safety Systems

End Users Covered:

- Automotive OEMs
- Fleet Operators
- Telecommunications Providers
- Software Developers

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK

+357 96 030922
info@marketpublishers.com

- Italy
- France
- Spain
- Rest of Europe

Asia Pacific

- Japan
- China
- India
- Australia
- New Zealand
- South Korea
- Rest of Asia Pacific

South America

- Argentina
- Brazil
- Chile
- Rest of South America

Middle East & Africa

- Saudi Arabia

+357 96 030922
info@marketpublishers.com

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:

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

+357 96 030922
info@marketpublishers.com

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

## 5 GLOBAL VEHICLE CYBERSECURITY MARKET, BY SECURITY TYPE

5.1 Introduction
5.2 Network Security
5.3 Application Security
5.4 Cloud Security
5.5 Endpoint Security
5.6 Wireless Security

## 6 GLOBAL VEHICLE CYBERSECURITY MARKET, BY PROPULSION TYPE

6.1 Introduction
6.2 Internal Combustion Engine (ICE) Vehicles
6.3 Electric Vehicles

## 7 GLOBAL VEHICLE CYBERSECURITY MARKET, BY VEHICLE TYPE

7.1 Introduction
7.2 Passenger Cars
7.3 Light Commercial Vehicles
7.4 Heavy Commercial Vehicles

## 8 GLOBAL VEHICLE CYBERSECURITY MARKET, BY APPLICATION

8.1 Introduction
8.2 Telematics Systems
8.3 Infotainment Systems
8.4 Powertrain Systems
8.5 Body Control & Comfort Systems
8.6 ADAS & Safety Systems

## 9 GLOBAL VEHICLE CYBERSECURITY MARKET, BY END USER

9.1 Introduction
9.2 Automotive OEMs
9.3 Fleet Operators
9.4 Telecommunications Providers
9.5 Software Developers

+357 96 030922
info@marketpublishers.com

## 10 GLOBAL VEHICLE CYBERSECURITY MARKET, BY GEOGRAPHY



## 11 KEY DEVELOPMENTS

+357 96 030922
info@marketpublishers.com



## 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: Vehicle Cybersecurity Market Forecasts to 2032 – Global Analysis By Security Type (Network Security, Application Security, Cloud Security, Endpoint Security, and Wireless Security), Propulsion Type, Vehicle Type, Application, End User, and By Geography.

Product link: https://marketpublishers.com/r/V0EE4A82165FEN.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/V0EE4A82165FEN.html