+357 96 030922
info@marketpublishers.com

Safety and Cybersecurity in Connected Mobility Market Forecasts to 2034 – Global Analysis By Solution Type (Software, Hardware and Services), Vehicle Type, Deployment, Security Layer and By Geography

https://marketpublishers.com/r/S27DAC696680EN.html
Date: March 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: S27DAC696680EN

Abstracts

According to Stratistics MRC, the Global Safety and Cybersecurity in Connected Mobility Market is accounted for $0.77 billion in 2026 and is expected to reach $1.79 billion by 2034 growing at a CAGR of 11.0% during the forecast period. In connected mobility environments, safety and cybersecurity serve as foundational elements as vehicles, infrastructure, and digital platforms share information in real time. Technologies such as ADAS, V2X communication, and remote software updates enhance operational safety while simultaneously increasing vulnerability to cyber risks. Ensuring protection demands strong data encryption, resilient system design, continuous monitoring, and timely software updates. Compliance with global regulations and security standards also plays a vital role in mitigating cyber attacks and data misuse. As transportation systems evolve toward automation and digital integration, embedding cybersecurity into system architecture safeguards users and sustains confidence in smart mobility solutions.

According to RunSafe Security’s 2025 Connected Car Cyber Safety & Security Index, a survey of 2,000 drivers found that less than one in five (19%) connected car drivers are very confident their vehicle is protected from cyberattacks, while 76% fear remote attacks could endanger lives.

Market Dynamics:

Driver:

+357 96 030922
info@marketpublishers.com

Rising adoption of connected and autonomous vehicles

The expanding deployment of connected and self-driving vehicles significantly fuels demand for advanced safety and cybersecurity solutions. These vehicles depend on integrated software platforms, sensor networks, V2X communication, and cloud-based services to function effectively. However, greater connectivity introduces vulnerabilities to cyberattacks and system intrusions. To address these risks, manufacturers and technology providers are prioritizing secure system architecture, encrypted communication channels, and proactive threat detection mechanisms. Strengthening cybersecurity frameworks helps safeguard vehicle operations, user data, and critical infrastructure, ultimately reinforcing trust and accelerating the adoption of intelligent mobility systems across global markets.

Restraint:

High implementation and integration costs

Elevated expenses related to deploying and embedding cybersecurity frameworks limit market expansion in connected mobility. Establishing secure software environments, advanced encryption protocols, and threat monitoring systems demands considerable capital outlay. Companies must further invest in regulatory compliance, vulnerability testing, and ongoing system upgrades. Smaller manufacturers often struggle to absorb these financial burdens, slowing innovation and adoption rates. Retrofitting older vehicle models with modern security features also raises technical and operational costs.

Opportunity:

Growth of smart city and intelligent transportation projects

The advancement of smart urban infrastructure programs offers promising opportunities for safety and cybersecurity solution providers. Intelligent transportation networks rely on real-time connectivity between vehicles and city systems, increasing the importance of secure communication channels. Protecting these integrated environments demands encrypted networks, identity management systems, and proactive monitoring capabilities. Public investments in digital mobility and infrastructure modernization enable cybersecurity companies to expand partnerships and service portfolios. As cities worldwide embrace connected transportation technologies, the need for scalable and resilient cybersecurity solutions is expected to grow substantially.

+357 96 030922
info@marketpublishers.com

Threat:

Increasing regulatory penalties and legal liabilities

Heightened regulatory scrutiny and expanding legal accountability represent serious risks for connected mobility providers. Authorities are implementing comprehensive cyber security mandates and strict data governance policies. Organizations that fail to adhere to these requirements may face substantial financial penalties and reputational damage. Furthermore, cyber incidents causing operational disruptions or safety hazards could trigger litigation and compensation claims. Navigating complex and evolving regulatory landscapes adds operational strain, making compliance management a critical yet challenging aspect of connected mobility cybersecurity strategies.

Covid-19 Impact:

The outbreak of COVID-19 created both challenges and opportunities for the connected mobility safety and cyber security sector. Early in the crisis, factory shutdowns, logistics interruptions, and chip shortages delayed vehicle manufacturing and technology integration. Budget constraints temporarily slowed new cybersecurity deployments. Nevertheless, the rapid shift toward digital operations, remote vehicle monitoring, and cloud-enabled services expanded connectivity requirements. Greater dependence on digital ecosystems increased exposure to cyber risks, prompting stronger emphasis on security frameworks. As the automotive industry rebounded, companies intensified efforts to embed robust cybersecurity and safety measures into software-centric mobility systems, supporting sustained market growth.

The passenger cars segment is expected to be the largest during the forecast period

The passenger cars segment is expected to account for the largest market share during the forecast period because of widespread connectivity adoption and large-scale manufacturing. These vehicles commonly feature ADAS, digital dashboards, telematics units, V2X communication systems, and remote update capabilities, increasing exposure to cyber risks. Protecting these interconnected systems necessitates advanced encryption, intrusion detection, and secure platform management. Rising customer expectations for intelligent, safe, and seamlessly connected driving experiences continue to drive cyber security implementation. With ongoing advancements in software-driven automotive design, passenger cars continue to lead demand for integrated safety and cyber security solutions.

+357 96 030922
info@marketpublishers.com

The vehicle-to-cloud segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the vehicle-to-cloud segment is predicted to witness the highest growth rate, driven by rising dependence on cloud infrastructure. Connected vehicles increasingly utilize remote servers for analytics, performance monitoring, digital services, and software updates. This growing reliance on external platforms expands potential cyber risk exposure, necessitating advanced protection mechanisms. Strong encryption standards, secure APIs, identity verification systems, and continuous monitoring are essential to safeguard cloud interactions. As digital ecosystems become central to automotive innovation, investment in secure Vehicle-to-Cloud frameworks is rapidly increasing across the global mobility industry.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, supported by rapid technological advancements and widespread deployment of connected vehicles. The region's well-developed IT ecosystem, strong presence of automotive innovators, and proactive adoption of intelligent transportation systems contribute to its leading position. Automakers and mobility service providers prioritize robust cybersecurity integration to address increasing digital connectivity. Regulatory enforcement and heightened focus on privacy compliance further encourage investment in secure vehicle platforms. Rising customer expectations for safe and digitally enabled driving experiences continue to accelerate the adoption of advanced cyber security measures throughout the North American mobility landscape.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, fueled by accelerating connected vehicle adoption and urban transport development. Expanding smart mobility projects, increasing use of autonomous technologies, and cloud-based vehicle services amplify the need for advanced cyber security measures. Government initiatives, investment in intelligent transport infrastructure, and collaboration between automakers and tech firms promote secure digital vehicle ecosystems. Heightened consumer focus on safety and privacy enhances demand for protective solutions. These trends position Asia-Pacific as a high-growth market for innovative and comprehensive connected mobility cyber security offerings.

+357 96 030922
info@marketpublishers.com

Key players in the market

Some of the key players in Safety and Cybersecurity in Connected Mobility Market include AUMOVIO, BlackBerry Limited, Vector Informatik GmbH, Dellfer, Karamba Security, Argus Cyber Security, Siemens, GuardKnox, Nvidia, NXM Labs, Irdeto, NCC Group, Intertrust, Exein, Synopsys, Bureau Veritas, Continental AG and Robert Bosch GmbH

Key Developments:

In January 2026, AUMOVIO and Amazon Web Services, Inc. (AWS), an Amazon.com, Inc. company announced a strategic agreement to help accelerate the development of safer, smarter self-driving vehicles, as well as establishing AWS as AUMOVIO's preferred cloud provider for autonomous driving development.

In October 2025, Continental AG has reached a deal with former managers that will see their insurance pay damages between 40 million and 50 million euros ($46.7 million-$58.3 million) in connection with the diesel scandal. The deal with insurers, subject to shareholder approval, covers only some of the total damages of 300 million euros.

In July 2024, Robert Bosch has agreed to acquire Johnson Controls and Hitachi's residential ventilation businesses for $8 billion, in what will be the German engineering group's largest takeover to date. Bosch said Johnson's heating, ventilation and air conditioning (HVAC) business for residential and small commercial applications would strengthen its Bosch Home Comfort arm, boosting the division's sales to 9 billion euros ($9.8 billion) from 5 billion euros currently.

Solution Types Covered:

- Software
- Hardware
- Services

Vehicle Types Covered:

+357 96 030922
info@marketpublishers.com

- Passenger Cars
- Commercial Vehicles
- Two-Wheelers & Micro-Mobility
- Off-Highway & Special Vehicles

Deployments Covered:

- Private Vehicles
- Shared Mobility
- Fleet & Logistics Operators
- Public Transport Systems

Security Layers Covered:

- In-Vehicle Systems
- Vehicle-to-Cloud
- Vehicle-to-Infrastructure
- User Interfaces

Regions Covered:

- North America
  - United States
  - Canada

+357 96 030922
info@marketpublishers.com

- 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

+357 96 030922
info@marketpublishers.com

- 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

+357 96 030922
info@marketpublishers.com

- 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)

+357 96 030922
info@marketpublishers.com

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

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+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 Rest of the World (RoW) Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Safety and Cybersecurity in Connected Mobility Market Forecasts to 2034 – Global Analysis By Solution Type (Software, Hardware and Services), Vehicle Type, Deployment, Security Layer and By Geography

Product link: https://marketpublishers.com/r/S27DAC696680EN.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/S27DAC696680EN.html