# Automotive Cybersecurity Market to Reach USD 14.2 Bn by 2035, Growing at 11.9% CAGR | Transparency Market Research

*Rising connectivity, ADAS, OTA updates, and V2X drive demand for strong automotive cybersecurity to combat growing cyber threats.*

Automotive Cybersecurity

WILMINGTON, DE, UNITED STATES, September 26, 2025 / EINPresswire.com/ -- As vehicles transition into highly sophisticated, connected, and software-driven machines, cybersecurity has become one of the most pressing challenges in the automotive industry. With the rise of autonomous technologies, electric vehicles (EVs), over-the-air (OTA) updates, and Vehicle-to-Everything (V2X) communication systems, cars have transformed into digital platforms on wheels. This evolution, while enhancing safety and convenience, has simultaneously created an expanded attack surface for cybercriminals. Consequently, the global automotive cybersecurity market, valued at USD 3.8 billion in 2024, is projected to grow at a CAGR of 11.9% from 2025 to 2035, reaching USD 14.2 billion by the end of 2035.

> As vehicles become more connected and software-driven, cybersecurity is no longer optional—it is essential for safety, trust, and compliance.”
>
> *Transparency Market Research*

Market Overview: Automotive cybersecurity refers to the protection of vehicle systems, networks, and onboard technologies against cyber threats. It encompasses everything from infotainment systems and electronic control units (ECUs) to telematics platforms and cloud services. The goal is to ensure confidentiality, integrity, and availability of vehicle systems throughout the vehicle lifecycle—from design to post-sales support.

This sector has gained heightened importance with the advent of software-defined vehicles (SDVs), advanced driver assistance systems (ADAS), and connected mobility services. Regulatory

frameworks such as UNECE WP.29 and ISO/SAE 21434 have also compelled automakers and suppliers to implement stringent cybersecurity measures.

Key Drivers of Market Growth

1. Rise of Software-Defined and Autonomous Vehicles
Modern cars rely heavily on ECUs, real-time AI processing, and OTA updates, making cybersecurity vital. As manufacturers shift toward SDVs, the number of potential vulnerabilities multiplies. Ensuring secure software, encrypted communications, and intrusion detection becomes essential to maintain safety and consumer trust.

2. Growing Incidence of Cyberattacks
High-profile cases of remote hacking—where attackers controlled critical functions such as brakes and steering—have spotlighted the urgency of robust automotive cybersecurity. Attackers increasingly target infotainment systems, telematics, and cloud platforms, exposing sensitive data and creating risks to both safety and privacy.

3. Regulatory Push
Governments worldwide are imposing strict compliance standards. The UNECE WP.29 regulations and ISO/SAE 21434 standard mandate comprehensive cybersecurity measures across the entire automotive lifecycle, driving significant market adoption.

4. Rise of Connected and Electric Vehicles
EVs and connected cars rely extensively on cloud platforms, wireless networks, and AI systems, which necessitate advanced cybersecurity frameworks. Consumer demand for secure, connected driving experiences further accelerates adoption.

Full Market Report available for delivery. For purchase or customization, please request here – https://www.transparencymarketresearch.com/sample/sample.php?flag=S&rep_id=86060

Key Players and Industry Leaders

The market is highly competitive, with global technology providers, automotive OEMs, and cybersecurity specialists shaping its landscape. Prominent players include:

- Aptiv
- Bosch Mobility Solutions
- Capgemini
- Continental AG (Argus Cyber Security)
- Cybellum Ltd.
- ETAS
- Infineon Technologies AG
- Karamba Security
- Lattice Semiconductor

- Microchip Technology
- NXP Semiconductors
- SBD Automotive Ltd
- Panasonic Holdings Corporation
- RunSafe Security
- STMicroelectronics
- Samsung Electronics Co., Ltd
- Synopsys
- Tata ELXSI
- Upstream Security Ltd
- Vector Informatik GmbH

These companies are focusing on bug bounty programs, secure chipsets, intrusion detection systems (IDS), encrypted gateways, AI-powered monitoring tools, and partnerships to expand their offerings and ensure regulatory compliance.

Recent Developments

- August 2025 – RunSafe Security released its Connected Car Cyber Safety & Security Index, highlighting that only 19% of drivers felt confident in their vehicle's cybersecurity. Importantly, 87% of drivers stated cybersecurity influenced purchasing decisions, with 35% willing to pay more for secure cars.
- October 2024 – Panasonic Automotive Systems expanded its VERZEUSE™ suite, offering container-based virtualization, automated threat analysis tools, and compliance-ready solutions for ISO/SAE 21434 and UN-R155.

Such advancements signal the industry's commitment to fortifying vehicles against rapidly evolving threats.

New Opportunities and Challenges

Opportunities:
- AI-Powered Cybersecurity Solutions: Leveraging artificial intelligence and machine learning for predictive threat detection.
- Cybersecurity-as-a-Service (CaaS): Cloud-based platforms enabling continuous monitoring and real-time defense.
- 5G Integration: With V2X communications, the role of cybersecurity will expand significantly in safeguarding mobility ecosystems.

Challenges:
- High Cost of Implementation: Developing and deploying advanced security frameworks raises vehicle production costs.
- Evolving Threat Landscape: Cybercriminals continuously adapt, requiring ongoing investments in R&D.
- Interoperability Issues: Integration of security solutions across diverse platforms, suppliers, and regions remains complex.

Latest Market Trends

- Adoption of Secure OTA Updates: Automakers are prioritizing safe OTA software patches to fix vulnerabilities remotely.
- Collaborative Ecosystems: OEMs, Tier-1 suppliers, and IT companies are forming alliances for shared cybersecurity frameworks.
- Hardware Security Modules (HSMs): Increasing integration of dedicated hardware for encryption and secure processing.
- Consumer-Driven Demand: Rising customer awareness of data privacy and vehicle safety is pushing cybersecurity into the spotlight of vehicle purchase decisions.

Future Outlook

Analysts anticipate that by 2035, cybersecurity will be a standard feature in all vehicles rather than a differentiating factor. As connected and autonomous cars proliferate, intrusion detection systems, encrypted communications, secure gateways, and AI-driven defense mechanisms will be indispensable.
Additionally, the EV revolution, combined with 5G-powered V2X networks, will further elevate cybersecurity's role in safeguarding both vehicles and the broader mobility ecosystem. Companies that can balance regulatory compliance, cost efficiency, and innovative technologies will emerge as industry leaders.

Market Segmentation

By Component:
- Software
- Hardware
- Services

By Deployment:
- In-Vehicle
- External Cloud Services

By Security Type:
- Cloud Security
- Endpoint Security
- Wireless Network Security
- Others

By Vehicle Type:
- Passenger Vehicles
  - Hatchback

- Sedan
- Utility Vehicle
- Light Commercial Vehicles
- Heavy Duty Trucks
- Buses & Coaches

By Propulsion:
- IC Engine Vehicles (Gasoline & Diesel)
- Electric Vehicles
  - Battery Electric (BEVs)
  - Plug-in Hybrid Electric (PHEVs)
  - Fuel-Cell Electric Vehicles (FCEVs)

By Application:
- ADAS & Safety
- Body Control & Comfort
- Communication Systems
- Infotainment
- Powertrain Systems
- Telematics
- On-Board Diagnostics (OBD)
- Electronic Control Units (ECUs)

Regional Insights

- North America: Leading the market due to strong regulatory frameworks, presence of top tech companies, and growing connected vehicle adoption. Agencies such as NHTSA and CISA are actively pushing vehicle cybersecurity initiatives.
- Europe: Benefits from strict UNECE regulations and a strong base of premium automakers investing in advanced security features.
- Asia Pacific: Rapidly growing due to China, Japan, and South Korea's dominance in EV production and connected vehicle adoption.
- Latin America & Middle East & Africa: Emerging markets where growing digitization and government regulations are expected to create new opportunities.

Why Buy This Report?

Purchasing a comprehensive Automotive Cybersecurity Market Report provides:
1. In-depth Market Analysis: Covering global trends, growth drivers, restraints, and emerging opportunities.
2. Detailed Forecasts: Reliable data projecting market growth up to 2035.
3. Segmentation Insights: Covering component, vehicle type, deployment, propulsion, application, and regional breakdowns.

4. Competitive Landscape: Profiling leading companies with insights into their strategies, product portfolios, and financial performance.
5. Regulatory Updates: Information on compliance requirements such as ISO/SAE 21434 and UNECE WP.29.
6. Consumer Insights: Analysis of how end-user demand and awareness influence market trends.
7. Strategic Guidance: Helping automakers, suppliers, and IT firms make informed decisions to stay ahead in a rapidly evolving market.

Browse More Trending Research Reports:

Acoustic Vehicle Alerting System (AVAS) Market: https://www.transparencymarketresearch.com/acoustic-vehicle-alerting-system-market-report.html
Automotive Drive Shaft Market: https://www.transparencymarketresearch.com/automotive-drive-shafts-market.html
Facial Injectables Market: https://www.transparencymarketresearch.com/facial-injectables-market.html
Tire Pressure Monitoring System Market: https://www.transparencymarketresearch.com/tire-pressure-monitoring-system-automotive-market.html

About Transparency Market Research

Transparency Market Research, a global market research company registered at Wilmington, Delaware, United States, provides custom research and consulting services. Our exclusive blend of quantitative forecasting and trends analysis provides forward-looking insights for thousands of decision makers. Our experienced team of Analysts, Researchers, and Consultants use proprietary data sources and various tools & techniques to gather and analyses information.

Our data repository is continuously updated and revised by a team of research experts, so that it always reflects the latest trends and information. With a broad research and analysis capability, Transparency Market Research employs rigorous primary and secondary research techniques in developing distinctive data sets and research material for business reports.

Contact:

Transparency Market Research Inc.
CORPORATE HEADQUARTER DOWNTOWN,
1000 N. West Street,
Suite 1200, Wilmington, Delaware 19801 USA
Tel: +1-518-618-1030
USA - Canada Toll Free: 866-552-3453
Website: https://www.transparencymarketresearch.com

Email: sales@transparencymarketresearch.com
Follow Us: LinkedIn| Twitter| Blog | YouTube

Atil Chaudhari
Transparency Market Research Inc.
+1 518-618-1030
email us here
Visit us on social media:
LinkedIn
Instagram
YouTube
X

---

This press release can be viewed online at: https://www.einpresswire.com/article/852788159

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2025 Newsmatics Inc. All Right Reserved.