Future of Automotive Cybersecurity Market PDF | Market Share & Opportunities 2025–2032

Automotive cybersecurity market surges as connected cars rise, driving demand for data safety and secure mobility solutions.

AUSTIN, TX, UNITED STATES, August 26, 2025 /EINPresswire.com/ -- Market Size and Growth

Global automotive cybersecurity Market reached US$ 3,370.00 million in 2024 and is expected to reach US$ 12,601.67 million by 2032, growing with a CAGR of 18.3% during the forecast period 2025-2032.

Automotive Cybersecurity Market

The global automotive cybersecurity market is experiencing a transformative phase, driven by the rapid adoption of connected and software-defined vehicles (SDVs) across passenger and commercial fleets. In 2024, the National Highway Traffic Safety Administration (NHTSA) reported that over 80% of newly sold vehicles in the US are equipped with advanced telematics, infotainment, and driver-assistance systems, significantly increasing the potential attack surface for cyber threats. Governments worldwide are stepping up regulatory oversight, with UNECE WP.29 R155/156 regulations now adopted in 64 countries, requiring manufacturers to implement Cybersecurity Management Systems (CSMS) and secure over-the-air (OTA) update capabilities across the vehicle lifecycle.

> The U.S. and Japan drive automotive cybersecurity growth as rising connected car adoption fuels a market surpassing billions by 2031.”
>
> *DataM Intelligence 4Market Research LLP*

Get a Sample PDF Of This Report (Get Higher Priority for Corporate Email ID):-
https://www.datamintelligence.com/download-sample/automotive-cybersecurity-market

Strategic Cybersecurity Initiatives and Government-Led Programs

1. US Department of Transportation (DOT) and NHTSA Guidelines: NHTSA's 2024 Cybersecurity Best Practices for Modern Vehicles mandate continuous monitoring, risk assessment, and mitigation measures for connected vehicle systems, emphasizing the integration of cybersecurity into design, production, and operation.

2. Automotive Information Sharing and Analysis Center (Auto-ISAC): Auto-ISAC has documented over 1,200 cyber incidents affecting connected vehicles between 2021–2024, highlighting the critical need for standardized threat intelligence sharing and preventive measures.

3. International Cooperation: The European Union and Japan have launched joint initiatives to harmonize cybersecurity protocols for SDVs, focusing on software integrity, secure data exchange, and collaborative incident response mechanisms.

Emerging Trends: AI, OTA Updates, and SDV Security

1. Artificial Intelligence (AI)-Enabled Security: Leading manufacturers are deploying AI-driven anomaly detection systems in SDVs to identify real-time threats across vehicle networks, enhancing response times and reducing potential damage from cyberattacks.

2. Over-the-Air Updates: Governments are mandating that OTA systems include robust encryption and authentication mechanisms to ensure updates cannot be hijacked or manipulated by malicious actors.

3. Autonomous Vehicle Integration: As autonomous vehicles become more prevalent, cybersecurity frameworks are evolving to address risks in sensor fusion, decision-making algorithms, and vehicle-to-everything (V2X) communications.

North America: Leading the Charge in Connected Vehicle Security

Regulatory Oversight and Government Initiatives

• In North America, the United States stands at the forefront of automotive cybersecurity, largely due to proactive regulatory measures and significant investments in connected vehicle technologies. The National Highway Traffic Safety Administration (NHTSA) has been instrumental in shaping the cybersecurity landscape for modern vehicles. In its 2024 report, NHTSA highlighted the increasing complexity of vehicle systems and the corresponding rise in cybersecurity risks. To address these challenges, NHTSA has issued comprehensive guidelines emphasizing the integration of cybersecurity measures throughout the vehicle lifecycle, from design to decommissioning.

• Furthermore, the US Department of Transportation (DOT) has been actively involved in research and development efforts aimed at enhancing the security of connected vehicle communications. Initiatives include the development of secure communication protocols and the testing of advanced detection systems to safeguard against potential cyber threats.

Key Players:

• Denso Corporation
• CENTRI
• Arxan Technologies Inc.
• Lear Corporation
• Delphi Automotive PLC
• Argus Cyber Security
• Harman International Industries Inc.
• SBD Automotive & NCC Group
• Intel Corporation
• Trillium Inc.

Buy Now & Unlock 360° Market Intelligence:- https://www.datamintelligence.com/buy-now-page?report=automotive-cybersecurity-market

Industry Adoption and Compliance

• The automotive industry in North America has responded to these regulatory frameworks by adopting stringent cybersecurity measures. Manufacturers are increasingly aligning their development processes with international standards such as ISO/SAE 21434, which provides guidelines for cybersecurity risk management in road vehicles. Compliance with these standards ensures that vehicles are designed with robust security features, including secure over-the-air (OTA) update capabilities and resilient communication networks.

Europe: Harmonizing Standards and Strengthening Regulations

UNECE WP.29 Regulations

1. In Europe, the United Nations Economic Commission for Europe (UNECE) has played a pivotal role in standardizing automotive cybersecurity practices. The WP.29 regulations, specifically UN Regulation No. 155 (R155) and UN Regulation No. 156 (R156), mandate that all new vehicles meet stringent cybersecurity requirements. These regulations necessitate the implementation of a Cybersecurity Management System (CSMS) and secure software update mechanisms to protect vehicles from cyber threats.

2. As of July 2024, these regulations have been adopted by 64 countries, including all European Union member states. The enforcement of these regulations signifies a unified approach to

vehicle cybersecurity across the region, ensuring that vehicles are equipped with the necessary safeguards against evolving cyber threats.

ISO/SAE 21434 Adoption

1. In conjunction with UNECE regulations, the adoption of ISO/SAE 21434 has been widespread among European automakers. This standard provides a comprehensive framework for managing cybersecurity risks throughout the vehicle's lifecycle. It covers aspects such as threat analysis, risk assessment, and the implementation of countermeasures to mitigate potential vulnerabilities.

2. Manufacturers are increasingly integrating these standards into their development processes, ensuring that cybersecurity is a fundamental consideration in the design and production of vehicles. This proactive approach not only enhances vehicle security but also fosters consumer confidence in the safety of connected and autonomous vehicles.

Asia-Pacific: Embracing Cybersecurity in Smart Mobility

Government Mandates and Investments

• In the Asia-Pacific region, countries like Japan, South Korea, and China are making significant strides in integrating cybersecurity measures into their automotive sectors. Governments are implementing stringent data protection laws and cybersecurity standards to safeguard connected vehicles from potential cyber threats.

• For instance, Japan has allocated substantial funds towards developing advanced cybersecurity solutions for the automotive industry, focusing on protecting autonomous driving systems and connected vehicle networks. Similarly, South Korea and China are investing in research and development to enhance the security features of their domestic vehicle fleets, aligning with international cybersecurity standards to ensure the safety of their connected vehicle ecosystems.

Market Segmentation:

By Security: (Communication networks, Electronic Systems, Software, ExternalInterfaces, Hardware)

By Vehicle Type: (PassengerVehicles, Commercial Vehicles)

By Protection & Monitoring: (External Interface, In-Vehicle networks, In-Vehicle State of Health, Security Field, Air Software & Vehicle Update)

By Application: (ADAS & Safety System, Telematics System, Power strain System, Infotainment

System, Body Control & Comfort System)

By Region: (North America, Latin America, Europe, Asia Pacific, Middle East, and Africa)

Conclusion

The global automotive cybersecurity landscape is rapidly evolving, with significant advancements in regulatory frameworks, industry standards, and government initiatives across North America, Europe, and Asia-Pacific. As vehicles become more connected and autonomous, the emphasis on robust cybersecurity measures is paramount to ensure the safety and privacy of consumers.

Through continued collaboration between governments, regulatory bodies, and the automotive industry, a secure and resilient automotive ecosystem can be established, capable of addressing the emerging challenges of the digital age. The commitment to cybersecurity in vehicle design and operation will not only protect consumers but also pave the way for the future of smart and connected mobility.

Why Choose this Automotive Cybersecurity PR Report?

• Government & Regulatory Insights: Full coverage of UNECE, NHTSA, and international cybersecurity mandates for connected and autonomous vehicles.
Innovation Spotlight: AI-driven threat detection, OTA security, and SDV-specific cybersecurity solutions highlighted.
• Geopolitical & Regional Analysis: Focus on North America, Europe, and Asia-Pacific government-led initiatives shaping adoption.
• Actionable Strategies: Guidance for automakers and Tier-1 suppliers to align with compliance, risk mitigation, and technology adoption.

Expert Analysis: Insights from leading automotive cybersecurity specialists and government compliance officers.

Stay ahead in a rapidly evolving automotive landscape, where connectivity, autonomy, and global regulations are redefining vehicle safety and cybersecurity standards.

Request New Version of Full Report: https://www.datamintelligence.com/enquiry/automotive-cybersecurity-market

Latest People Also Ask for Related Reports By DataM Intelligence:

Automotive Wet Friction Materials Market

Automotive Battery Thermal Management System Market

Sai Kiran
DataM Intelligence 4Market Research LLP
+1 877-441-4866
sai.k@datamintelligence.com
Visit us on social media:
LinkedIn
X
