+357 96 030922
info@marketpublishers.com

Automotive Cyber Security Market Assessment, By Component [Software, Services], By Organization Size [Large Enterprises, Small & Medium Enterprises], By Vehicle Type [Passenger Vehicle, Commercial Vehicles], By Propulsion Type [ICE, Electric, Hybrid], By Application [ADAS & safety, Infotainment, Body electronics, Powertrain, Telematics], By Region, Opportunities and Forecast, 2016-2030F

https://marketpublishers.com/r/A626FADFDDD9EN.html
Date: February 2025
Pages: 228
Price: US$ 4,500.00 (Single User License)
ID: A626FADFDDD9EN

Abstracts

Global automotive cyber security market has experienced significant growth in recent years and is expected to maintain a strong pace of expansion in the coming years. With projected revenue of approximately USD 5.03 billion in 2022, the market is forecasted to reach a value of USD 15.2 billion by 2030, displaying a robust CAGR of 14.8% from 2023 to 2030.

Automotive cybersecurity protects vehicles and their electronic systems from cyber threats and attacks. With the increasing connectivity and complexity of modern vehicles, including features such as infotainment systems, advanced driver assistance systems (ADAS), autonomous driving capabilities, and vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, the need for robust cybersecurity measures in the automotive industry has become paramount. The automotive cyber security market involves the technologies, solutions, and services designed to protect vehicles and their electronic systems from cyber threats and attacks. As vehicles become more connected and autonomous, the automotive industry's need for robust cybersecurity measures has grown significantly.

+357 96 030922
info@marketpublishers.com

According to Upstream’s 2023 Global Automotive Cybersecurity Report, the leading cyberattack vectors 2022 encompassed various areas, with telematics and application servers at the forefront, accounting for 35% of attacks. Following closely, remote keyless entry systems encountered 18%, 14% in electronic control units, 12% automotive and smart mobility APIs, 8% infotainment systems, 6% mobile applications, and 4% EV charging infrastructure.

Increasing Adoption of Connected Vehicles

The increasing adoption of connected vehicles in the automotive industry has significantly impacted the cybersecurity market. As vehicles become more connected, with features such as infotainment systems, wireless communication, telematics, and vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, the attacking surface for potential cyber threats and vulnerabilities has expanded. Connected vehicles introduce new avenues for cyberattacks, including remote hacking, unauthorized access to vehicle systems, data breaches, and more. As the components within a vehicle become interconnected, they become a potential entry point for malicious acts. The adoption of connected vehicles has facilitated the implementation of secure OTA software updates. These updates are crucial for addressing vulnerabilities and applying patches to protect vehicles against emerging threats.

For example, in May 2023, VicOne introduced its innovative Smart Cockpit Protection Solutions designed specifically for OEMs to safeguard their customers' data privacy. This comprehensive offering from VicOne comprises two key components: the Smart Cockpit Security App, which ensures the privacy of data within the in-vehicle infotainment (IVI) systems, and the Smart Cockpit Mobile SDK (software development kit), which provides robust protection for OEM car companion apps. By integrating these solutions with VicOne's existing cybersecurity offerings, OEMs can benefit from a robust and multi-layered cybersecurity defense spanning from the fundamental system level to the application layer.

Electric Vehicles to be More Vulnerable to Cyber Attacks

The growing adoption of electric vehicles (EVs) has introduced a heightened vulnerability to cyber-attacks. As the automotive industry shifts towards electric propulsion systems, the increased reliance on complex software, connectivity, and data exchange makes EVs more susceptible to cyber threats. EVs heavily depend on sophisticated software systems to manage power distribution, battery management, regenerative braking, and other critical functions. The complexity of this software

+357 96 030922
info@marketpublishers.com

increases the attack surface, providing more entry points for potential cyber intrusions. Some EVs have advanced driver assistance systems (ADAS) and autonomous capabilities. These features rely on extensive sensor data and communication, making them a potential target for manipulation or disruption.

For example, in September 2022, Elektrobit and Argus Cyber Security introduced the EB zoneo SwithCore Shield. This innovative solution integrates embedded intrusion detection and prevention (IDP) capabilities into advanced network management systems for next-generation vehicles. This collaborative effort presents a compact embedded module featuring the Argus Ethernet Intrusion Detection and Prevention System (IDPS). The robust cybersecurity safeguard is designed for automotive ethernet networks and seamlessly integrated as automotive-grade switch firmware within the vehicle's electrical and electronic (E/E) architectures.

Implementation of ADAS Propels Market Growth

Implementing Advanced Driver Assistance Systems (ADAS) capabilities is a driving force behind the growth of the automotive cybersecurity market. As vehicles are implementing advanced ADAS technologies, which include features like adaptive cruise control, lane departure warning, automatic emergency braking, and more, the complexity and connectivity within vehicles are exponentially rising. This complexity opens new avenues for potential cyber threats and vulnerabilities that could have compromised the safety and functionality of these systems. As a result, the automotive industry is greatly emphasizing cybersecurity measures to safeguard ADAS and other vehicle systems.

For instance, in September 2022, Electric automaker XPeng unveiled China's first advanced driver assistance system (ADAS) tailored for urban driving scenarios. The company officially introduced its City Navigation Guided Pilot (City NGP) ADAS. This system is currently undergoing pilot testing in Guangzhou, initially featuring on the P5 electric sedan—a direct competitor of the Tesla Model 3. The deployment of City NGP will be facilitated through an over-the-air update mechanism.

Government Initiatives

Government initiatives play a significant role in shaping the global automotive cybersecurity market. They are implementing and promoting various policies of network security at the global level. These initiatives often focus on data security, privacy regulations, and standardization to build trust and confidence among businesses and

+357 96 030922
info@marketpublishers.com

consumers. Government authorities are investing in cyber security infrastructure development, offering incentives, and creating supportive regulatory frameworks to encourage cloud adoption and stimulate innovation.

Recent research indicates that cybersecurity in the automotive sector will prompt substantial investments, surging from USD 4.9 billion in 2020 to USD 9.7 billion in 2030. The initiative of the UN Regulations framework is poised to drive innovation and foster economic prospects for a wide range of stakeholders, including suppliers, IT companies, specialized niche enterprises, and startups, especially within the software development and services market.

Impact of COVID-19

The COVID-19 pandemic significantly impacted various industries, including the cybersecurity sector in the automotive industry. The pandemic increased cyberattacks and security breaches as hackers exploited the uncertainties and vulnerabilities introduced by remote work arrangements and increased online activities. The pandemic disrupted supply chains, manufacturing, and research and development efforts, leading to delays in deploying new vehicles and technologies. This negatively impacted the integration of cybersecurity measures for vehicles and systems. Furthermore, the pandemic underscored cross-industry collaboration's importance in addressing cybersecurity challenges. As a result, companies and governments have increased their collaborative efforts to strengthen cybersecurity in the automotive sector, especially in Asia Pacific.

Impact of the Russia-Ukraine War

Russia-Ukraine war notably impacted the global automotive cyber security market. The conflict has led to concerns about data privacy, security, and geopolitical instability, prompting businesses to re-evaluate their automotive cyber security infrastructure. Automotive companies are becoming increasingly cautious about storing sensitive data in regions affected by the conflict, leading to a potential shift in cyber security service providers through cloud solutions for better control and risk management. Moreover, the war has disrupted internet connectivity in certain areas, affecting the reliability and accessibility of security cloud services. Additionally, geopolitical tensions have raised concerns about data sovereignty and compliance with international regulations. As a result, businesses focus on diversifying their cyber security infrastructure and exploring alternative markets to mitigate potential risks, ensuring uninterrupted operations and data protection.

+357 96 030922
info@marketpublishers.com

Key Players Landscape and Outlook

The automotive cyber security market is witnessing a swift growth trajectory due to the increasing emphasis placed by companies worldwide on establishing advanced automotive cyber security infrastructure. Furthermore, the market expansion is greatly facilitated by the establishment of proper cloud infrastructure, along with significant investments made by companies to enhance research and development resources, engage in collaboration projects, bolster marketing efforts, and expand distribution networks. These factors collectively contribute to the rapid expansion of the market.

In February 2023, Elektrobit unveiled the immediate release of EB tresos 9, the latest version of its top-tier foundational software. The software empowers automotive manufacturers and suppliers to create effective electronic control units (ECUs) aligned with the latest AUTOSAR standard. The new iteration accommodates AUTOSAR R20-11, while seamlessly integrating the remarkable onboard intrusion-detection functionalities found in Argus CAN IDPS. Notably, Argus Cyber Security, recognized with the CES 2023 innovation award, is behind the development of these industry-leading intrusion-detection capabilities.

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

7. AUTOMOTIVE CYBER SECURITY MARKET OUTLOOK, BY REGION, 2016-2030F

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

8. MARKET MAPPING, 2022

9. MACRO ENVIRONMENT AND INDUSTRY STRUCTURE

10. MARKET DYNAMICS

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Automotive Cyber Security Market Assessment, By Component [Software, Services], By Organization Size [Large Enterprises, Small & Medium Enterprises], By Vehicle Type [Passenger Vehicle, Commercial Vehicles], By Propulsion Type [ICE, Electric, Hybrid], By Application [ADAS & safety, Infotainment, Body electronics, Powertrain, Telematics], By Region, Opportunities and Forecast, 2016-2030F

Product link: https://marketpublishers.com/r/A626FADFDDD9EN.html

Price: US$ 4,500.00 (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/A626FADFDDD9EN.html