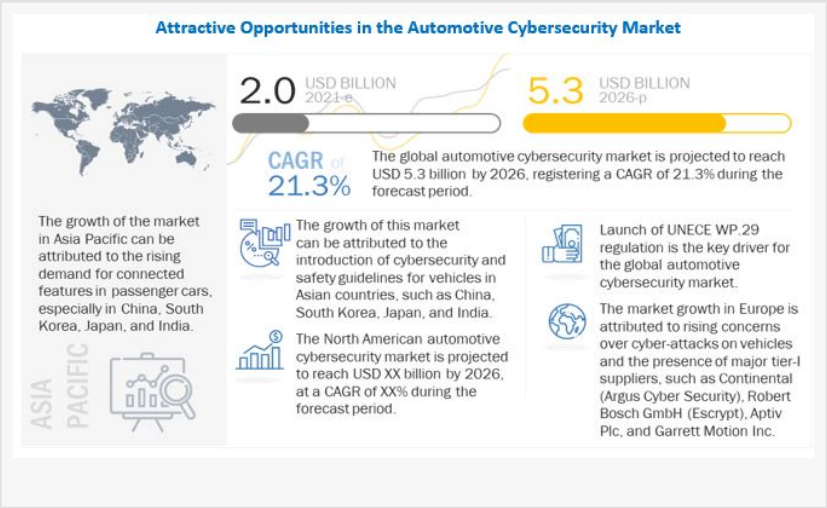
Automotive Cybersecurity Market: Statistics & Growth Dynamics to 2026

Increasing incidents of cyber-attacks on vehicles and massive vehicle recalls by OEM have increased awareness about automotive cybersecurity among OEMs globally



NORTHBROOK, ILLINOIS, UNITED STATES, June 21, 2022 /EINPresswire.com/ -- The global Automotive Cybersecurity Market is projected to grow by USD 5.3 billion by 2026 from USD 2.0 billion in 2021, at a CAGR of 21.3%.

The automotive cybersecurity market, however, is expected to witness a significant boost in 2022 owing to the increase in vehicle production in different countries, the launch of UNECE WP.29 regulation as well as various government regulations that have compelled automotive OEMs to install additional safety systems in vehicles for better safety.

Growth Driver: Increased use of electronics per vehicle and a growing number of connected cars

In recent times, electrification has helped to reduce the overall weight of a vehicle. Thus, the demand for electronics has increased at a rapid pace in the automotive industry. The increasing use of electronics has made vehicles more vulnerable to cyberattacks. The electronic components for various applications such as telematics, infotainment, powertrain electronics, body electronics, communication electronics, and ADAS systems are prone to cyberattacks. Hence, stakeholders have started to invest in cybersecurity solutions to make robust electronic platforms for vehicles.

The development of vehicle connectivity has made a vehicle more prone to cyberattacks. The in-vehicle applications are getting more complex with the increase in the use of ECU and software with 30 million to 40 million lines of code. Thus, the security of each software code line is essential. According to industry experts, a large share of new cars would be connected to

networks by 2022. Therefore, many OEMs and security solution providers are taking steps to counter cyber threats. However, every secured design would not guarantee full security over a period. Hence, there is a need for the consistent implementation of security codes in connected vehicles. Accordingly, OEMs are focusing on minimizing the chances of security lags and making software patches more secure through the cloud. Hence, the market for automotive cybersecurity is expected to grow with the rise in the number of connected cars in the coming years.

The software segment is expected to dominate the global automotive cybersecurity market.

In terms of market share in the global automotive cybersecurity industry, the hardware to software ratio per vehicle is around 20:80. This is expected to change over the years with variations in hardware prices. Cybersecurity software inside the vehicle requires the implementation of a number of security functionalities such as secure protocols, identity and access management, intrusion detection, and abstraction layers for crypto functions. These functionalities are then used by the functional ECUs to secure communications and avoid the creation of backdoors. Therefore, the software segment is expected to hold the largest share in the automotive cybersecurity market during the forecast period globally.

ADAS & safety systems are expected to dominate the automotive cybersecurity market during the forecast period

The ADAS & safety segment is expected to dominate the automotive cybersecurity market during the forecast period. ADAS comprises ECUs/DCUs utilized to control airbags, collision warning, and tire pressure systems. The market growth in this segment is largely driven by the growing incorporation of ECUs/DCUs that control ADAS and related functionality. Government mandates and increasing awareness about vehicle safety are also expected to fuel the demand for ADAS & safety systems across the globe. Europe and North America are estimated to witness significant demand for ADAS and safety systems. Regulatory bodies of the EU have mandated forward-collision warning systems and autonomous emergency braking systems in all new vehicles by 2022. Regulatory bodies in the US are also encouraging OEMs to make forward-collision warning systems and autonomous emergency braking systems standard features in all their new vehicles by the end of 2022. The government of India also plans to make ADAS features such as Electronic Stability Control (ESC) and Autonomous Emergency Braking (AEB) mandatory for all passenger cars by 2022-23. Therefore, government mandates, along with the increasing awareness of vehicle safety, are expected to fuel the demand for ADAS & safety systems. Thereby, the demand for automotive cybersecurity solutions is also expected to grow at a rapid pace during the forecast period globally.

The Asia Pacific is expected to be the largest market during the forecast period

The Asia Pacific is estimated to account for the largest market share in 2021, followed by Europe and North America. The rising awareness of active and passive safety features among people and increasing sales of mid-sized and luxury vehicles are the key factors driving the automotive cybersecurity market in the Asia Pacific. Several OEMs have shifted their automobile manufacturing plants to emerging countries because of low labour costs, ease of doing business, and the availability of raw materials. Several well-known semiconductor companies have their manufacturing hubs in the Asia Pacific region as well. This helps them maintain an effective supply chain of their products for the automakers.

Moreover, the growing sales of V2X-equipped vehicles and significant growth in ride-sharing industries are likely to increase the demand for automotive cybersecurity solutions in the Asia Pacific region. OEMs in Japan and South Korea, such as Hyundai, Kia, Nissan, Honda, and Toyota, are focused on the development of self-driving cars. This is further expected to spur the demand for related cybersecurity solutions. Similarly, in the Indian market, OEMs such as MG Motor, Kia, and Mahindra have already started offering car models with level 1/2 features, which would further support the demand for cybersecurity solutions in the coming years. Apart from this, Asia Pacific is home to some of the top players in the automotive cybersecurity market, such as Autotalks and AutoCrypt. Growing electric vehicle adoption and an increasing number of vehicles with connected car features would boost the need for automotive cybersecurity in the region. All these factors put together are expected to drive the Asia Pacific automotive cybersecurity market during the forecast period.

Europe shows significant growth potential for the automotive cybersecurity market

Europe presents a big growth opportunity for the automotive cybersecurity market as the regulations related to safety issues have become stringent. As this region is an early adopter of regulations and mandates for safety standards and technologies, these stringent safety standards have driven the adoption of advanced ADAS and safety features such as eCall and collision warning. This, in turn, supports the demand for automotive cybersecurity solutions in Europe. Also, the evolution of digital technologies, such as robotics, the Internet of Things, artificial intelligence, high-performance computers, and powerful communication networks, in the connected car segment is expected to increase the demand for automotive cybersecurity solutions in Europe. Therefore, the increasing demand for connected cars equipped with V2Xand other modern technologies is likely to drive the automotive cybersecurity market in this region. Additionally, the development of an intelligent transportation system (ITS) would also drive the automotive cybersecurity market in Europe.

The automotive cybersecurity market comprises significant manufacturers such as Continental AG (Germany), Robert Bosch GmbH (Germany), Harman International (US), DENSO Corporation

(Japan), Aptiv PLC (Ireland), Garrett Motion Inc. (Switzerland), Renesas Electronics Corporation (Japan), Karamba Security (Israel), SafeRide Technologies (Israel), Arilou Technologies (Israel), GuardKnox Cyber Technologies Ltd. (Israel), Upstream Security Ltd. (Israel), etc.

Recent Developments:

1. In November 2021, NXP Semiconductors collaborated with Ford Motor Company to deliver enhanced driver experiences, convenience, and services like over-the-air updates across its global fleet of vehicles, including the 2021 Ford F-150 pickup, Mustang Mach-E, and Bronco SUVs.
2. In October 2021, Renesas Electronic Corporation acquired Celeno Communications (Israel) to develop more advanced Wi-Fi connectivity capabilities to deliver end-to-end connectivity solutions for clients and access points.
3. In September 2021, Harman International collaborated with Renault (France) to provide the Harman Kardon sound system to the Renault Mégane E-TECH 100% electric that is expected to be launched in 2022.
4. In July 2021, ETAS Korea, a subsidiary of Robert Bosch GmbH, signed a partnership agreement with Suresoft Tech Co., Ltd. (South Korea) to offer consulting services and solutions related to cybersecurity testing of in-vehicle systems to Korean automotive manufacturers and suppliers.
5. In July 2021, NXP Semiconductors collaborated with Moter Technologies, Inc. (US) to combine its new S32G2 high-performance automotive processors with MOTER's insurance data science expertise and software. This is expected to enable vehicle data monetization with new and improved automotive insurance services.
6. In May 2021, ESCRYPT, a subsidiary of ETAS Inc, which is a subsidiary of Robert Bosch GmbH, partnered with Alyne GmbH and KPMG to offer joint expertise in developing the Product Security Organisation Framework (PROOF).
7. In April 2021, Elektrobit collaborated with SUSE (Germany) to supply its EB corbos Linux OS to car makers and Tier 1 suppliers in China.
8. In May 2021, Harman International introduced an end-to-end 5G Testing Lab for 5G CP devices in India. It is expected to equip technology providers like device manufacturers, chipmakers, Telcos, etc., to execute a variety of protocols and functional tests. This also helps validate and examine applications in a real 5G radio environment.
9. In December 2020, Elektrobit selected ArcherMind Technology (Nanjing) Co., Ltd. as a value-added distributor in China for reselling their software products as well as providing engineering and customer support services to their customers.

Mr. Aashish Mehra
MarketsandMarkets™ INC
+ +1 888-600-6441
email us here

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.