China Automotive Cybersecurity Market Forecast 2024-2032

Market Report | 2024-08-12 | 141 pages | Inkwood Research

AVAILABLE LICENSES:

- Single User Price $1100.00
- Global Site License $1500.00

Report description:

KEY FINDINGS
The China automotive cybersecurity market is predicted to prosper at a CAGR of 18.18% over the forecast period of 2024-2032. It is set to reach a revenue of $2935.67 million by 2032.
MARKET INSIGHTS
China is a global leader in automotive production, which makes its automotive cybersecurity market the largest in Asia. This prominence is attributed to the country's immense production scale, increasing adoption of electric vehicles, advanced in-vehicle infotainment (IVI) systems, and strong governmental backing. The vast automotive industry in China creates a significant demand for robust cybersecurity measures to protect against evolving digital threats.
In December 2023, China's Ministry of Transport introduced new trial guidelines for autonomous vehicle (AV) services, which include robotaxis, self-driving trucks, and robo-buses. Developed after a comprehensive 16-month public consultation, these guidelines aim to standardize operational rules and enhance safety measures for AVs. The regulations stipulate that autonomous buses can only operate on enclosed or simple-condition roads, robotaxis are restricted to controlled traffic environments, and robo-trucks are limited to well-maintained highways or favorable traffic conditions. Operators must secure permits for public transport services, and AVs are required to have clear road awareness labels.
Additionally, any over-the-air software updates must comply with safety regulations established by the Ministry of Industry and Information Technology (MIIT). The MIIT is also working on establishing mandatory national standards for automobile information security. In June 2023, a call for public feedback on these standards was issued, with a deadline of July 5, 2023. The objective is to finalize and release the first version of these standards by mid-2024, with implementation set for mid-2025. These standards are designed to bolster cybersecurity in the automotive sector, ensuring that both vehicles and their components meet stringent security requirements.
Furthermore, in June 2023, the Chinese State Council announced a regulatory framework to enhance the quality of the country's charging infrastructure. This framework addresses critical issues such as standardization, construction quality, and design imbalances. The aim is to develop a comprehensive, high-quality, and cybersecurity charging network by 2030, aligning with China's broader objectives for sustainable and secure automotive infrastructure. These regulatory and infrastructural improvements highlight China's commitment to advancing automotive cybersecurity and supporting the rapid growth of its automotive sector.
SEGMENTATION ANALYSIS

The China automotive cybersecurity market segmentation incorporates the market by vehicle propulsion type, offering, and security type. The security type segment is further segregated into in-vehicle security and connected vehicle security. In-vehicle security is crucial for automotive cybersecurity, focusing on protecting the internal systems and components of a vehicle to ensure safe and secure operation.

A key element in this domain is the security of Electronic Control Units (ECUs), which are responsible for managing essential functions like braking, steering, and engine control. Securing ECUs involves implementing secure bootloaders to prevent unauthorized software installation and using encryption to protect sensitive data stored and processed by these units. These measures are vital for safeguarding against malicious attacks and ensuring the integrity of vehicle operations.

Another important aspect of in-vehicle security is network protection. Modern vehicles contain numerous ECUs that need to communicate securely within the vehicle's network. This requires the use of firewalls to block unauthorized access and data exchanges between ECUs. Authentication protocols are essential for verifying and trusting communication between these units, preventing unauthorized devices from accessing or manipulating data. Additionally, Intrusion Detection and Prevention Systems (IDS/IPS) play a critical role in monitoring the vehicle's internal networks for suspicious activities and mitigating threats to maintain the security of critical functions.

Secure software development practices are integral to minimizing vulnerabilities in in-vehicle software. This involves employing static and dynamic analysis tools to identify and address potential weaknesses early in the development process. Regular updates and patching are also crucial to ensure that software remains current with the latest security fixes. By focusing on ECU security, robust network protection, IDS/IPS deployment, and rigorous software development practices, automakers can significantly enhance the cybersecurity of modern vehicles, protecting them from evolving cyber threats.

Connected network security is essential for safeguarding a vehicle's interactions with external networks, such as cellular and Wi-Fi connections, to protect against threats like man-in-the-middle attacks. This includes securing the Telematics Unit (TMU), which manages the collection and transmission of critical vehicle data, such as location, diagnostics, and driver behavior. Ensuring the security of the TMU involves preventing unauthorized access and data breaches through the implementation of secure communication protocols, encryption, and authentication methods to maintain data privacy and integrity.

Another key aspect is vulnerability management, which entails the proactive identification and patching of weaknesses in the software and firmware related to the vehicle's connected systems. Regular updates and security patches are vital to address potential vulnerabilities before they can be exploited. Additionally, Information and Event Management (SIEM) systems are used to monitor and analyze real-time data from vehicles, detecting suspicious activities and potential threats. Advanced diagnostics and remote monitoring further enhance security by allowing for early detection of issues and providing valuable information for responding to cyberattacks effectively.

COMPETITIVE INSIGHTS

Some of the leading players in the China automotive cybersecurity market include Infineon Technologies AG, NXP Semiconductors NV, Robert Bosch GmbH, Continental AG, etc.

NXP Semiconductors NV, headquartered in the Netherlands, is a leading Dutch multinational specializing in semiconductor design and manufacturing. NXP became independent from Koninklijke Philips NV after Philips sold 80 percent of its stake. The company provides technology solutions for automotive, industrial, IoT, mobile, and communication markets, as well as for government applications, including RFID tags and electronic passports.

Table of Contents:

SCOTTS INTERNATIONAL

China Automotive Cybersecurity Market Forecast 2024-2032

Market Report | 2024-08-12 | 141 pages | Inkwood Research

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User Price	$1100.00
	Global Site License	$1500.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2025-06-26
		Signature	