United States Automotive Cybersecurity Market Forecast 2024-2032

Market Report | 2024-08-12 | 145 pages | Inkwood Research

AVAILABLE LICENSES:

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

Report description:

KEY FINDINGS
The United States automotive cybersecurity market is projected to grow at a CAGR of 18.00% over the forecast period of 2024-2032. It is set to reach a revenue of $2834.41 million by 2032.
MARKET INSIGHTS
The automotive cybersecurity market in the United States is experiencing significant growth fueled by regulatory advancements, technological innovations, and increasing consumer concerns about data privacy and security. Several key developments in 2023 have underscored the crucial role of cybersecurity in the automotive sector.
In March 2023, the Federal Highway Administration (FHWA) introduced the National Electric Vehicle Infrastructure (NEVI) Standards and Requirements. This regulation requires compliance with ISO 15118 and Plug and Charge capabilities for publicly accessible EV chargers. The new standards aim to standardize and secure EV charging infrastructure, enhancing consumer data protection and ensuring the cybersecurity of charging stations and power grids.
The US Department of Commerce's National Institute of Standards and Technology (NIST) also made strides with the finalization of NIST IR 8473, a guidance document addressing cybersecurity risks associated with extremely fast charging infrastructure. This framework provides a comprehensive strategy for protecting the EV charging ecosystem against a wide range of cyber threats, recognizing the vulnerabilities in interconnected charging networks.
In August 2023, the California Privacy Protection Agency (CPPA) initiated an enforcement action focused on the extensive data collected by connected vehicles. This move highlights the increasing focus on data privacy within the automotive industry, pushing original equipment manufacturers (OEMs) to ensure transparency in data collection practices and compliance with data management regulations.
The market is also driven by the rapid advancement of connected and autonomous vehicle technologies, which require advanced cybersecurity measures to mitigate potential cyber threats. Effective industry collaboration and partnerships are crucial for developing and implementing robust cybersecurity solutions to protect these technologies.
Increased investment in research and development is further propelling market growth. This funding supports the innovation and enhancement of cybersecurity technologies, ensuring they can effectively address the evolving threat landscape faced by connected and autonomous vehicles. Collectively, these developments reflect a strong commitment within the automotive industry to address complex cybersecurity challenges. The market continues to evolve, amped by regulatory changes, technological advancements, and an increased focus on data privacy and security.

SEGMENTATION ANALYSIS

The United States automotive cybersecurity market segmentation incorporates the market by vehicle propulsion type, offering, and security type. The offering segment is further bifurcated into hardware and software. As vehicle technology progresses, the complexity of electrical and electronic systems within smart vehicles also increases. A software-defined vehicle (SDV) relies on centralized computers and sophisticated software stacks to manage a wide range of functions, from engine performance to infotainment systems. To operate these advanced systems effectively and efficiently, robust and secure hardware modules are essential.

The Hardware Bill of Materials (HBOM) is a critical technical document that outlines the hardware components used in a vehicle. This includes Electronic Control Units (ECUs), Telematics Control Units (TCUs), infotainment systems, gauge clusters, Controller Area Network (CAN) bus controllers, and IoT devices, each sourced from various suppliers and supply chains. As the number of ECUs and other electronic systems in vehicles rises, so does the potential attack surface for cyber threats. Therefore, automakers and suppliers must ensure that each hardware component adheres to rigorous security standards to prevent vulnerabilities. Industry stakeholders are increasingly focusing on developing hardware solutions with integrated security features, such as embedded security modules, cryptographic processors, secure boot mechanisms, and hardware-based intrusion detection systems. By embedding security within the hardware, a strong foundation is established to protect vehicle systems from cyber threats. As automotive systems become more reliant on advanced electronics and connectivity, the importance of secure hardware components will continue to grow.

Likewise, the Software Bill of Materials (SBOM) plays a critical role in enhancing cybersecurity within the automotive industry. It functions as a dynamic technical document that details the software components, libraries, and dependencies present in both vehicle hardware and software. When combined with the Hardware Bill of Materials (HBOM), the SBOM provides a comprehensive view of supply chains, enabling greater transparency and traceability to address vulnerabilities in both hardware and software systems.

As Over-The-Air (OTA) updates become standard in the automotive landscape, the SBOM must remain dynamic and continuously updated. This ongoing adaptability ensures that vulnerabilities are addressed in real time through new updates and patches, even after vehicles leave the factory. Additionally, the scope of SBOMs has expanded with the advent of Software-Defined Vehicles (SDVs), now encompassing charging points, networks, and third-party applications for smart mobility. This complexity requires meticulous management to secure the entire ecosystem effectively.

COMPETITIVE INSIGHTS

Some of the leading players in the United States automotive cybersecurity market include HARMAN International Industries Inc, Aptiv PLC, Upstream Security Ltd, etc.

Harman International Industries Inc, headquartered in Connecticut, is a leading American multinational company specializing in connected car technology, lifestyle audio innovations, professional audio and lighting solutions, and digital transformation. Operating globally across major regions, including the Americas, Asia-Pacific, and Europe, Harman was acquired by Samsung in 2017. Since then, it has functioned as an independent subsidiary of Samsung Electronics Co Ltd.

Table of Contents:

SCOTTS INTERNATIONAL

United States Automotive Cybersecurity Market Forecast 2024-2032

Market Report | 2024-08-12 | 145 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	2025-05-07
		Signature	