Cybersecurity For Cars - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Cybersecurity For Cars Market size is estimated at USD 3.06 billion in 2024, and is expected to reach USD 6.60 billion by 2029, growing at a CAGR of 16.66% during the forecast period (2024-2029).

The advent of connected cars and increasing demand for a relevant solution in passenger vecles is driving the need for cybersecurity, as more and more attacks are being carried out on connected cars. According to Upstream Auto, a cybersecurity solutions provider for the automotive industry, the auto industry might face a loss of USD 24 billion over the next five years due to cyberattacks.

Key Highlights
-Automotive cybersecurity involves complex systems that continuously analyze and monitor vehicle data for any signs of unauthorized access or malicious activity. These advanced systems employ technologies like intrusion detection and prevention systems (IDPS), anomaly detection algorithms, secure communication protocols, and over-the-air updates. The emergence of machine learning algorithms has extended new possibilities for detecting unknown or zero-day attacks in real time by analyzing patterns in vast amounts of data generated by vehicles.
-The dynamic nature of the connected vehicle features is significantly influencing the demand for cybersecurity. With every new connected entity or late service for connected cars, a new attack vector is also created from which the vehicle's security can be compromised.
-Major automotive players worldwide have opted for state-of-the-art cyber-security technologies such as blockchain, 5G, and artificial intelligence for security risks like malfunctions or cyber-attacks. However, with the technology growing, automotive cyber-security is also witnessing newer trends like Quantum Cryptography (QC) - borne out of the application of Vehicle Anti-theft Systems and quantum physics, Cryptographic Hash Functions (CHF) - providing improved security in private and public

blockchains.
-One major challenge is the complexity of modern vehicles. Today's cars have various electronic control units (ECUs), each responsible for multiple functions such as safety features, engine control, and infotainment systems. These ECUs communicate with each other and external devices through different networks, making securing every entry point from potential attacks challenging.
-With the outbreak of COVID-19, the automotive industry was one industry that negatively affected end-users. This also negatively impacted the demand for the cybersecurity market for cars. After initial supply and manufacturing disruptions, the automotive industry is experiencing a demand shock with an uncertain recovery timeline due to shelter-in-place regulations. With limited room to cut fixed costs, some OEMs needed more liquidity to power through a long period of missing revenues, which affected the market. According to Germany's Center for Automotive Research, the Western European automobile market will need about ten years to reach the size of 2019 again.

Cybersecurity For Cars Market Trends

Rising Security Threats as More Technologies Get Integrated Into Cars is Expected to Drive the Market

- The automotive industry faces a significant challenge due to digitalization, such as big data coming from multiple connected sources. It is only getting bigger, making it increasingly difficult to analyze and protect the connected car against cyber threats. The only way to cut through the data clutter and identify potential attacks is by leveraging artificial intelligence and machine learning technologies for behavioral analysis of the data.
- The rapid growth in cyberattacks on the connected automotive industry is increasing significantly. From 2010 to 2018, the cyberattacks in the automotive sector increased by six times, and black hat attacks exceeded the number of white hats in 2018. Upstream's 2022 Global Automotive Cybersecurity Report includes a detailed examination of over 900 automotive cybersecurity events, including the Advanced sophistication of 2021's 240+ attacks; 84.5% of automotive attacks were carried out remotely, and a staggering 40.1% of incidents focused on back-end servers attacks.
- In 2022, China published a trial regulation on vehicle data management to standardize vehicle data processing to protect the lawful rights and interests of individuals and organizations, protect national security and public interest, and promote rational development and utilization of data collected from automobiles.
- Additionally, According to the survey, China ICVs collect at least 10 TB of data per day, with the data including not only information about the driver and passengers' facial expressions, movements, sight, and voices but also the vehicle's geographic position, interior, and exterior environment, and use of the Internet of Vehicles (IoV) to strengthen vehicle data security management to prevent and fix these security issues and potential threats.
- As sensors increase rapidly in connected vehicles, hackers can potentially steal personally identifiable information (PII) from the vehicle's systems, such as personal trip and location data, entertainment preferences, and even financial information. The more manufacturers release mobile apps for communicating with cars, the more they become targets for adverse factors.
- In the case of the Nissan Leaf, a compact five-door hatchback battery electric vehicle (BEV), security testers demonstrated how they could gain unauthorized access to control the heated steering wheel, seats, fans, and aircon remotely. The increasing security vulnerabilities in the Android and iOS mobile operating systems are also becoming a concern. These instances would require a need for robust cybersecurity systems for cars.

North America is Expected to Hold Significant Market Share

- The National Highway Transportation Safety Administration (NHTSA) is one of the regulatory bodies in the region overseeing the

standards in security and safety of connected cars and released the 5G FAST Plan. This plan incorporates three key components: updating infrastructure policy, pushing more spectrum into the marketplace, modernizing outdated regulations, Vehicle-to-Everything (V2X) environment data exchange, and High-speed communications support Vehicle-to-Vehicle (V2V). Such data exchange allows autonomous vehicles to accept data beyond their onboard sensors' physical range.
- North America is one of the major automotive markets and holds a significant demand for connected cars; the region has observed a slump in demand similar to the global market since 2019; however, the demand is expected to pick up over the coming years. For instance, according to BEA, in 2021, the US's light-vehicle retail sales stood at 14.9 million units.
- Moreover, over the next three years, it is predicted that over 85% of the cars sold in the US are anticipated to be secured over the Internet. General Motors' OnStar platform was one of the country's most widely used software platforms and security systems. The country's growing adoption and penetration rates augment the demand for cybersecurity.
- Furthermore, US car sales of Japanese brands are up 8.6%, increasing their market share to 38.5%, the highest since 2010. European brands are up 10.5%, increasing their market share by 0.7 percentage points to 10.6%, a new yearly high and the first time they have reached double digits. South Korean brands surpass all others, increasing their market share by 1.5 percentage points to 9.9%.
- The demand for electronics in the automobile industry in this region has expanded rapidly. The increased usage of electronics in vehicles has rendered them more vulnerable to hackers. Cyberattacks are common on electronic components used in telematics, infotainment, powertrain electronics, body electronics, communication electronics, and ADAS systems. As a result, stakeholders across this region have begun investing in cybersecurity solutions to provide robust electronic automobile platforms.

Cybersecurity For Cars Industry Overview

The cybersecurity market for cars is highly competitive due to the presence of many small and large players operating in domestic and international markets. The market appears to be moderately concentrated, with the key players adopting strategies like product and service innovation to overcome the latest threats faced by automobiles continually. Some of the significant players in the market are Cisco Systems, Inc., Infineon Technologies, NXP Semiconductors NV, and Harman International Industries Inc., among others.

In January 2022, Visteon, a technology company servicing the mobility industry, announced the AllGo App Store as one of the latest solutions in its growing range of connected car technologies for the mobility sector at CES□ 2022. The AllGo App Store was created to fulfill the expanding global demand for secure and convenient access to app-based content in an innovative, connected cockpit.

In April 2022, Cisco and General Motors are collaborating to modernize and automate the development process for vehicle development data for performance testing, reducing time-to-market for commercially ready automobiles. Using Cisco's wireless network architecture for real-time, pre-production performance testing at GM Milford Proving Ground enables multiple GM test engineers to actively monitor several hundred data channels concurrently during a test run, observe vehicle operation parameters, and modify the test being run to optimize results.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Cybersecurity For Cars - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

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 License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	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	2026-03-03
		Signature	