Asia Pacific Automotive Cybersecurity Market Size to Hit US$ 4,944 million by 2030 – Astute Analytica

CHICAGO, UNITED STATES, November 21, 2022 /EINPresswire.com/ -- Asia Pacific automotive cybersecurity market revenue was US$ 1,288.6 million in 2021 and the market is forecast to reach US$ 4,944 million by 2030, growing at a compound annual growth rate (CAGR) of 16.1% during the forecast period from 2022 to 2030.

Request Sample Report at:
https://www.astuteanalytica.com/request-sample/asia-pacific-automotive-cybersecurity-market

Market Snapshot
The automotive cybersecurity sector protects the new generation of electronic software, data, and systems of smart cars. In addition, in order to cause potentially fatal crashes, hackers can steal personal information, including banking and social security numbers, and to make current and upcoming cars safer and more secure, many companies are creating cutting-edge automotive cybersecurity systems. For instance, Centri, an Autotech cybersecurity company situated in Washington, develops solutions for IoT-enabled devices in the automotive sector. The Centri IoTAS is a chip and mobile application that safeguards car sensors and information that helps vehicles understand important driver navigational preferences.

The modern automobile is highly sophisticated as it has several lines of software code, hundreds of microprocessors, and electrical control units. The modern car also consists of Bluetooth, find my car, Wi-Fi for remote starting, integrated cellular connectivity, and a number of other connected devices. Vehicle-to-infrastructure, vehicle-to-cloud, vehicle-to-everything, and vehicle-to-vehicle technology makes cars susceptible to hackers. The Asia Pacific automotive cybersecurity market is examined for the years 2017 to 2030, with the forecast years being 2022 to 2030 and the historic years being 2017 to 2020. The research report provides analysis that is explained over 12 chapters that together comprise 167 pages and 50 figures, and 28 substantial data tables.

Cyberattacks have been gradually rising over the past ten years. However, in this pandemic era, the rising popularity of work-from-home models and a lack of security precautions have led to a significant increase in cyberattacks globally. The two typical kinds of cyber-attacks are ransomware and malware attacks. Attacks by malware and ransomware are still more frequent in Asia Pacific nations, with rates that are 1.7 and 1.6 times higher than the rest of the world. The frequency of Ransomware attacks increased globally in 2018. Cyberattacks in the automotive industry have become more common as linked cars and digitalization have become more prevalent, by targeting the vehicle and damaging critical vehicle data, which causes owners to incur significant losses.

Market Influencing Factors

The market has experienced tremendous growth due to the proliferation of connectivity systems in automobiles. With the proliferation of linked cars, potential automotive attacks have moved beyond carjacking; instead, it is now possible to remotely hack vehicles. Most car owners use Bluetooth, Wi-Fi, or GPS to connect to their vehicles via their smartphones. Theft or malicious access to such data would put people's privacy at risk by gaining knowledge of their location in real time, recording their interactions with in-car entertainment, and even analyzing their behavior. Due to the fact that linked cars are part of a huge transportation system, there is also a risk of losing personal data, the entrance of erroneous information into a car or the ECU may malfunction, halting the entire system.

As companies get closer to semi- and completely driverless cars, automakers are also creating several intricate, active safety systems, such as lane departure warnings and active cruise control. For instance, Fiat Chrysler Automobiles (FCA) recently recalled 1.4 million vehicles following a potential remote breach. Among the impacted vehicles are the Jeep Grand Cherokee, Dodge Ram Pickup, Cherokee SUV, and others with 8.4-inch touchscreen car entertainment systems. As a result, the adoption of connected vehicles is likely to have an impact on the automotive cybersecurity market.

On the other hand, automotive cybersecurity is a challenging, dispersed, multi-stakeholder problem. It varies in the sense that the proficiency required to accurately assess the level of security of a particular IT system that is not always present in a single location. For instance, software developers for the automotive industry must produce software that interfaces with systems and components produced by numerous parties. It is also challenging for cybersecurity solution providers to defend and streamline their solutions using components/systems manufactured by multiple stakeholders, which limits the market growth.

Impact Analysis of COVID-19

COVID-19 had a negative effect on the automotive cybersecurity market. The outbreak has brought a crisis of unparalleled proportions for governments and businesses in the world. As a result of the COVID-19 outbreak in APAC, the entire country has been placed under lockdown,

requiring residents to stay home and forcing employers to permit employees to work from home. In order to be ready for a post-pandemic workplace, businesses globally are investing in networking technologies that can change to meet changing needs. Cybersecurity is now understood to be a crucial tactic for keeping organizations safe as they move virtual and online as they struggle to do so. Additionally, as cutting-edge technologies like blockchain, machine learning, and artificial intelligence reach maturity, cybersecurity investment will be seen as a key differentiator for companies that offer these services. There are four levels of impact analysis in the report: pre-covid (2017-2019), short-term (2020-21), mid-term (2022-24), and long-term (2025-30).

Browse Detailed Summary of Research Report: https://www.astuteanalytica.com/industry-report/asia-pacific-automotive-cybersecurity-market

Leading Companies
Some of the prominent companies operating in the Asia Pacific automotive cybersecurity market are:
Argus Cyber Security Ltd
Aptiv
ARILOU Automotive Cyber Security
Continental AG
Capgemini
Escrypt
Denso Corporation
ETAS
Guardknox Cyber-Technologies Ltd.
Elektrobit Automotive GmbH
Honeywell International Inc.
HARMAN International
Intel Corporation
Infineon Technologies AG
Lear Corporation
Karamba Security
Robert Bosch Gmbh
NXP Semiconductors
Saferide Technologies Ltd.
Rockwell Automation
Secunet
SBD Automotive Ltd.
TTTech Auto AG
Symantec Corporation
Vector Informatik GmbH.
UL LLC
Other Prominent Companies

Segmentation Outline

The Asia Pacific automotive cybersecurity market segmentation focuses on Offering, Applications, Vehicles, Security, Form, and Country.

By Offering
Hardware
Software
Services

By Application
ADAS & Safety
Body Electronics
Communication Systems
Infotainment
Powertrain
Telematics
Others

By Vehicles
Passenger cars
- Compact Passenger Cars
- Mid-sized Passenger Cars
- Premium Passenger Cars
- Luxury Passenger Cars

Commercial vehicle
- LCV
- HCV

Electric vehicle
- Battery Electric Vehicle (BEV)
- Fuel Cell Electric Vehicle (FCEV)
- Hybrid Electric Vehicle (HEV)
- Plug-in Hybrid Electric Vehicle (PHEV)

By Security
Endpoint
Application
Wireless Network

By Form
In-Vehicle
Cloud Services

By Country
China
Japan
India
Australia and New Zealand
ASEAN
Rest of Asia Pacific

Looking For Customization: https://www.astuteanalytica.com/ask-for-customization/asia-pacific-automotive-cybersecurity-market

About Astute Analytica
Astute Analytica is a global analytics and advisory company that has built a solid reputation in a short period, thanks to the tangible outcomes we have delivered to our clients. We pride ourselves in generating unparalleled, in-depth, and uncannily accurate estimates and projections for our very demanding clients spread across different verticals. We have a long list of satisfied and repeat clients from a wide spectrum including technology, healthcare, chemicals, semiconductors, FMCG, and many more. These happy customers come to us from all across the Globe. They are able to make well-calibrated decisions and leverage highly lucrative opportunities while surmounting the fierce challenges all because we analyze for them the complex business environment, segment-wise existing and emerging possibilities, technology formations, growth estimates, and even the strategic choices available. In short, a complete package. All this is possible because we have a highly qualified, competent, and experienced team of professionals comprising business analysts, economists, consultants, and technology experts. In our list of priorities, you-our patron-come at the top. You can be sure of best cost-effective, value-added package from us, should you decide to engage with us.

Aamir Beg
Astute Analytica
+1 888-429-6757
email us here
Visit us on social media:
Twitter
LinkedIn