

kaspersky

Driving automotive cybersecurity



Transportation
System Security

Introduction

IHS Markit forecasts that by 2023, worldwide sales of connected cars will reach 72.5 million units, up from 24 million units in 2015. That means almost 69% of passenger vehicles sold will be exchanging data with external sources, bringing new services and business models to bear in automotive markets*.

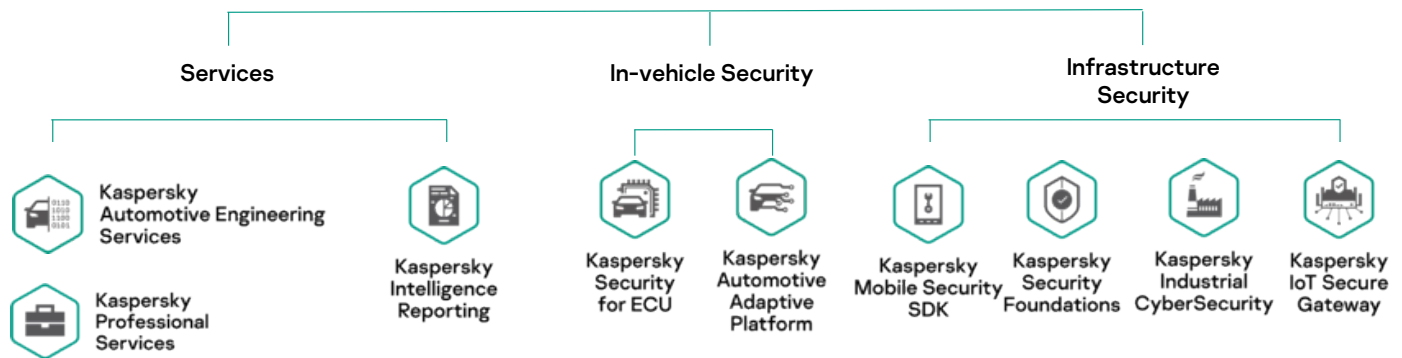
But there's still a long way to go to guarantee connected vehicles are safe and secure for passengers. For that to happen there needs to be a transformation in the multiple approaches used across the automotive industry.

Connected cars are more than just physical cars with digital technology – they are vehicles with connected infrastructures that include mobile management apps, OEM clouds, fleet management systems and more. As a result, we end up with connected car ecosystems with multiple entry points that are vulnerable to cyberattacks.

Kaspersky has introduced a set of products and services specifically designed to provide cybersecurity to connected cars and their infrastructures and to support the development of new mobility technologies, including autonomous, electric and shared technologies.



Kaspersky Transportation System Security



* lhsmarkit.com/topic/autonomous-connected-car.html

Uncover the Security Risks



Security Assessment

The Security Assessment service is the ideal starting point for addressing the cybersecurity agenda for connected cars and their infrastructures. It detects vulnerabilities, software architecture inconsistencies, and gaps in ECUs, hardware and software security mechanisms both in manufactured vehicles and future models and their components. Moreover, it makes it possible to identify problems across the entire connected car infrastructure, including mobile and web apps, V2X connectivity interfaces and other communications. Based on precise information about existing gaps and recommendations from global cybersecurity experts, it should be clear how to go about adapting your current security strategy, whether you manufacture cars, supply components for them or manage vehicle fleets on the aftermarket.



Penetration Testing

You shouldn't wait for a real cyberattack to find out if the security measures you have implemented are good enough to protect a connected car and its infrastructure. It makes more sense to conduct a simulated attack – either externally, internally or using so-called red teaming – in order to identify and demonstrate possible security gaps, mitigate risks in advance and ensure you're ready for an emergency. Kaspersky's expert team conducts penetration testing in accordance with international standards, including OSSTMM, PTES, OWASP, etc. In addition to a detailed technical report, the expert team also schedules a face-to-face follow-up meeting with your internal information security personnel.



Tailored Threat Intelligence Reporting

Brand reputation means a lot, especially in the automotive industry. Based on open-source data as well as analysis of underground activities, including on the deep web and Darknet, you can uncover evidence of any past or current attacks and spot signs of upcoming cyberattacks on your brand, supply chain or infrastructure and take timely countermeasures. You can also obtain information about the illicit activation and use of premium services, chip tuning and other activities around the world or in a particular region, in order to block and investigate fraudulent activity.

In-vehicle Cybersecurity products



Kaspersky Automotive Adaptive Platform

Kaspersky Automotive Adaptive Platform powered by KasperskyOS is an advanced specialized SDK. Its tools allow the creation of secure-by-design solutions for various electronic control units in smart cars, such as telecommunications, driver assistance systems and autopilot systems (HAD/ADAS), domain controllers, and digital cockpits. Applications based on this platform conform with the international AUTOSAR Adaptive standard and are updatable over the air via Uptane compatible solution. Built-in security mechanisms ensure multi-layered cybersecurity from the OS level, securing OTA services and integration with vehicle SOC.



Kaspersky Security for ECU

Kaspersky Security for ECUs (KSECU) provides control mechanisms and real-time intrusion detection for connected vehicles, their internal and external communications as well as the apps running on them. The solution incorporates vehicle fleet to vehicle security operation centers (VSOC), fleet management systems (FMS) and other security-related backend systems to achieve compliance with continuous monitoring requirements.

Tighten Infrastructure Protection



Mobile Security SDK

Whether it's an OEM app or a car-sharing app, it's part of the connected car ecosystem, and therefore capable of affecting security, including users' private data, if compromised. That's why the development of secure mobile applications must be treated as seriously as vehicle engineering. Kaspersky Mobile Security SDK provides a framework for developing mobile applications resistant to internal data leakage, app overlapping, app repackaging and other cyberthreats, providing mobility and fleet management enterprises with a practical tool to protect their businesses against fraudsters, while allowing car manufacturers to demonstrate an eye for detail.



Fraud Prevention

As part of the connected car ecosystem, websites and apps provide clients with access to premium services and contain personal data. With the ability to distinguish fake users from legitimate ones thanks to multiple machine learning techniques, you can prevent account takeover (ATO) incidents as well as protect your corporate network against malicious users. This not only minimizes reputational and financial risks but also cuts costs on multi-factor authorization for legitimate users.



Vehicle SOC

It won't be long until connected cars become an integral element in the smart city infrastructure. There are already dedicated vehicle SOCs collecting and processing security event data from multiple levels of the connected car infrastructure. Kaspersky is ready to help car manufacturers and mobility and fleet management enterprises create their own vehicle SOCs. In addition to data on applications, connected devices, communication events, geolocation and telemetry from the vehicle, the SOC teams can monitor anomalous events in web apps to identify correlations between events and detect cyberattacks in their early stages. Finally, Kaspersky can provide vehicle SOCs with advanced threat intelligence, acquired from over two decades of cybersecurity experience.

Why Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. With its deep threat intelligence and cybersecurity expertise gained over 22 years, Kaspersky is constantly developing security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. Protecting over 270,000 corporate clients worldwide, Kaspersky is considered the most trusted cybersecurity brand for business**.

With Kaspersky as a cybersecurity partner, automotive enterprises gain visibility into the entire connected vehicle ecosystem and an understanding of how to adjust their cybersecurity strategy. By integrating security into connected vehicles at every stage of their lifecycle and ensuring a secure drive for their clients, we're building a safer tomorrow.

Kaspersky – driving automotive cybersecurity!

** According to the results of 2018 report
The Boundaries of Trust: Privacy and Protection
in Cyberspace

Any questions?
Contact Kaspersky Automotive Security Services:
ktss@kaspersky.com

www.kaspersky.com

2022 AO Kaspersky Lab. All rights reserved.
Registered trademarks and service marks are the property of their
respective owners.