kaspersky

# Driving automotive cybersecurity

Transportation System Security

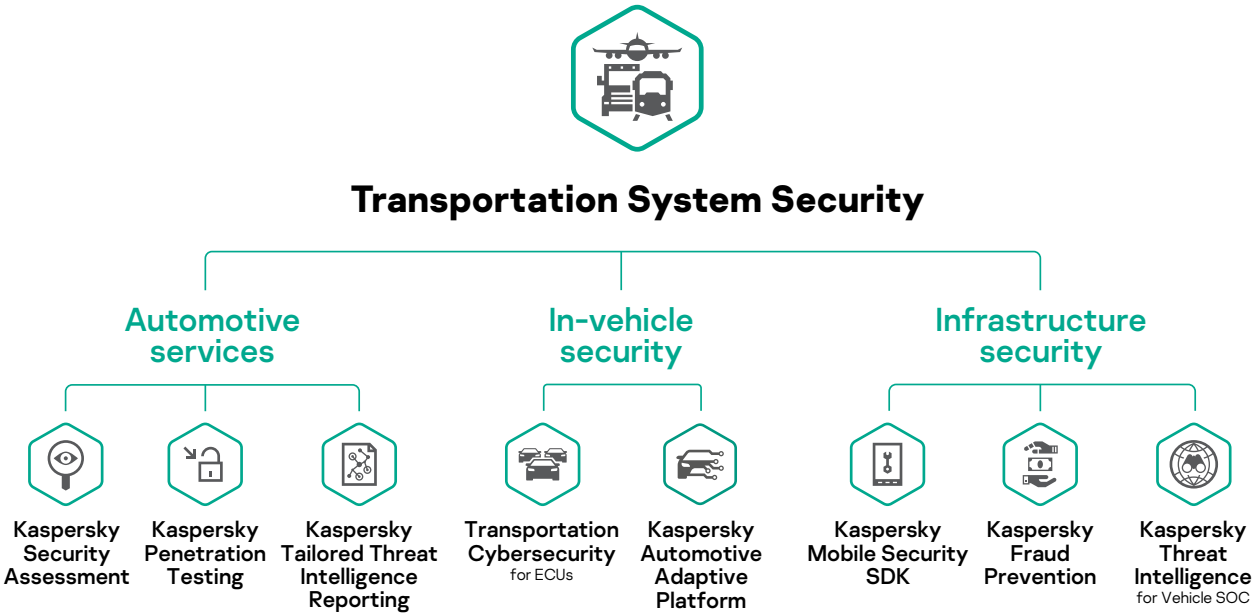
# Introduction

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.




* Ihsmarkit.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.

# Integrate Cybersecurity into the Vehicle

## Kaspersky Automotive Adaptive Platform

The Kaspersky Automotive Adaptive Platform is a newly developing standard for intelligent ECUs with the aim of bringing innovative technologies into the automotive world.
In partnership with AVL Software and Functions GmbH, Kaspersky is developing its own version of the Kaspersky Automotive Adaptive Platform, based on KasperskyOS with a strong focus on cybersecurity. This microkernel operating system implements MILS architecture and defines its own approach to control inter-process communications using a dedicated security engine – Kaspersky Security System. Unlike other security engines, it supports a whole range of formal security models simultaneously and allows security behavior to be specified with a high degree of precision, regardless of business logic.
For Tier 1 suppliers making their own platforms, we provide a set of complementary technologies, including Kaspersky Secure Hypervisor, Kaspersky Security System for different operating systems, Secure Boot, Secure Update, and Secure Audit to help those building safe, secure and reliable solutions.

## Transportation Cybersecurity for ECUs

With their multiple interfaces and cloud connections, infotainment, telematics, HPCs and other ECUs ensure proper and safe vehicle functioning. They are also responsible for the secure processing of sensitive data without influencing vehicle safety. ECUs can contain vulnerabilities and can be relatively easy for anyone – including attackers – to compromise and use as entry points into a connected car infrastructure. As a member of the AUTOSAR and GENIVI Alliance, Kaspersky has insights into next-gen vehicle infrastructures and the attendant security challenges. Kaspersky's security for ECUs is therefore capable of providing control mechanisms and real-time intrusion detection and prevention for connected devices, their internal and external communications as well as for the apps running on them.  Integration of ECU security technologies with multiple SIEM systems in vehicle security operation centers (SOCs) not only provides security officers with event logs but also gives them the tools to conduct incident analysis, threat hunting and further investigations. Moreover, when a new vulnerability is discovered at any stage of the vehicle lifecycle, it's possible to remotely shield it with a virtual patch, preventinga costly vehicle recall.

# 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**