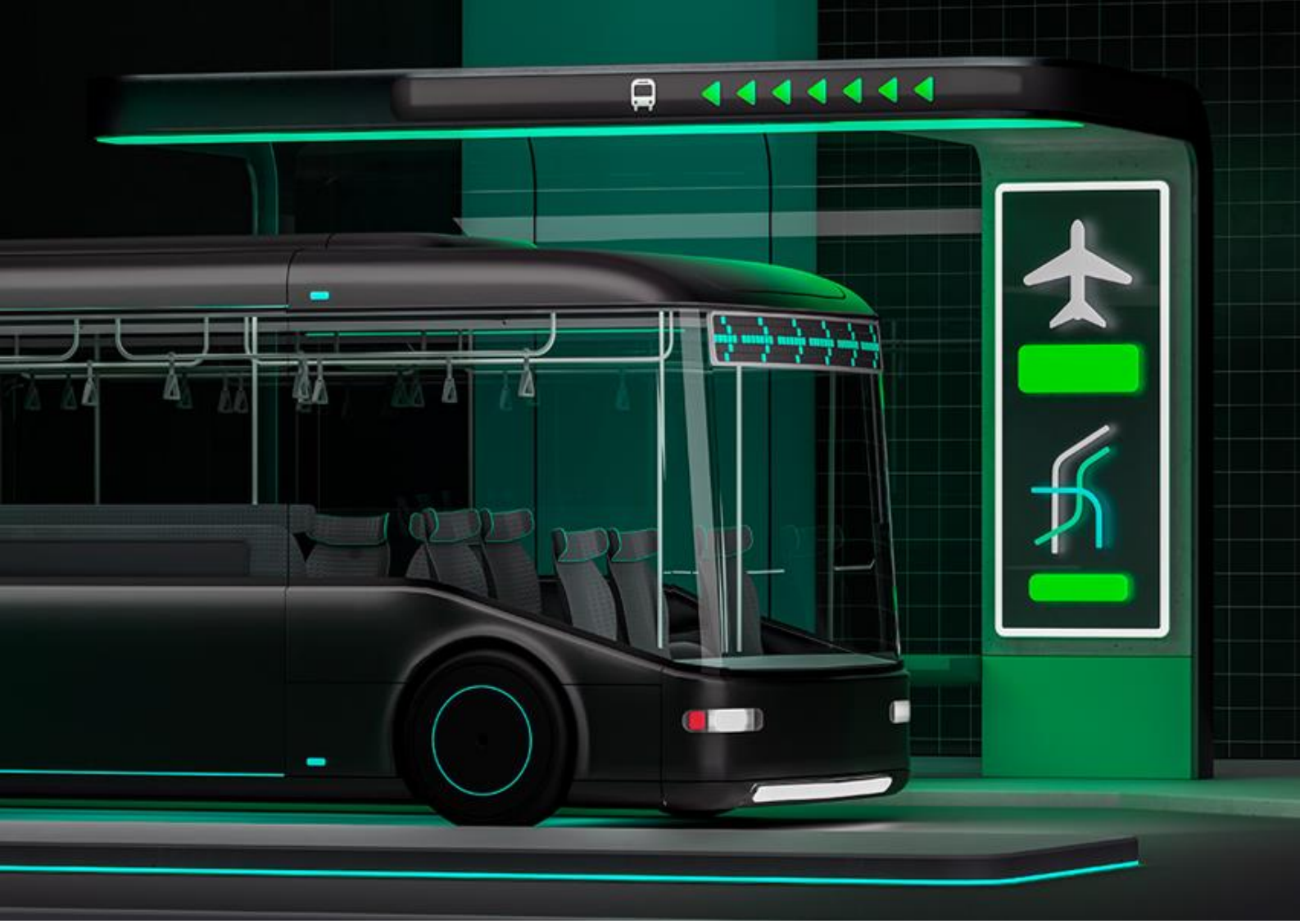


Building a safer future in Transportation

kaspersky bring on the future

Preventing a remake: Speed 2034

A fast-growing target for cybercriminals

$15,273 billion
projected global logistics market size by 2027

$33.6 billion
↗17% CAGR
estimated smart transportation market size by 2028

8.2 billion air travelers
predicted by the International Air Transport Association by 2037

In the 1994 hit action thriller Speed, Keanu Reeves and Sandra Bullock face the daunting task of saving all the passengers (including Bullock herself) on a bus that's been rigged by a terrorist to explode if its speed falls below 50 miles per hour. Fast forward 40 years, and the plot of a remake would more likely feature a hacker who's compromised the bus's electronic control systems — with equally nail-biting consequences.

Far-fetched as this might sound, there are numerous examples of vehicles having their electronic systems hacked by malicious actors. As long ago as 2015, researchers famously hacked a Jeep Cherokee, enabling them to take control of everything from the steering wheel, engine, transmission and braking system to windscreen wipers, air conditioning, door locks etc. This has been followed by a steady stream of incidents exposing the vulnerabilities of automotive systems, and damaging the reputations of the manufacturers involved.

According to research by Frost & Sullivan, by 2028 more than 85% of new vehicles will be internet-connected, and fully autonomous vehicles will be navigating public roads. To do so safely — and prevent Speed 2034 being commissioned — every single one of these vehicles will require cybersecurity solutions capable of preventing their potential vulnerabilities from being exploited.

But while the automotive segment is the focus of much current legislation designed to ensure this, similar considerations apply throughout the transportation industry — from freight and logistics to rail, shipping and air travel.

The transportation industry's transition to the digital world, and the avalanche of data that comes with 'digital fitness', attracts diverse cyberattacks threatening the security of individuals, as well as the integrity of transport operations. In this whitepaper, we'll therefore look at six key trends within the industry and the cybersecurity risks related to these.

Cybersecurity regulation in the transportation industry

Expansion of the autonomous vehicle market

The evolution of vehicle digital ecosystems

AI facilitates smarter route and delivery planning

Mobility as a Service (MaaS)

Vehicle telematics goes granular

Trend #1: The evolution of vehicle digital ecosystems

The transition to software-driven mobility providers

Until recently, a car manufacturer's role was to make a car, sell it, and service it through a network of physical centers. That has all changed, with car manufacturers rapidly transitioning into software-driven mobility providers producing smart devices on wheels. Underpinning this transition is a seamless, superfast, digitally-connected ecosystem coordinating numerous in-vehicle electronic systems to integrate the various services required by customers.

Customers now demand digital services that can be constantly improved, and new services added at the click of a mouse or tap of an app by providing software updates. Moving beyond digital vehicle retail and aftersales services, OEMs like Tesla and Volkswagen are leading the way with infotainment and enhanced digital vehicle services such as multimedia and autopilot. And service rentals based on monthly subscriptions are already becoming the norm, with up to a third of car manufacturers' revenues being received from services sales.

OEMs such as Volkswagen are spearheading the development of customer-centric digital ecosystems.

"By turning the vehicle into a software-based product, Volkswagen is setting the scene for new, data-based business models aimed at lowering entry barriers to individual mobility while offering very attractive service packages for the customers. Volkswagen thus aims to generate additional revenue over the service life of the vehicle through charging and energy services, through software-based functions that customers can reserve as needed, or through automated driving. "

Securing against vehicle digital ecosystem vulnerabilities

In tandem with the fast growth in connectivity and software-heavy systems comes an increase in vehicle ecosystem attack surfaces, and the consequent need to mitigate and protect connected vehicles from malware.

"A car today is basically a specialized computer — a 'cyber-brain' controlling the mechanics and electrics we traditionally associate with the word 'car' — the engine, the brakes, the turn indicators, the windscreen wipers, the air conditioner, and in fact everything else."

Frost & Sullivan estimates that the 56.5 million connected vehicles manufactured in 2022 will rise to 83.6 million by 2028, and that this presents the sector with significant security challenges:

By 2030, the vast majority of new vehicles will be internet-connected as standard. By then, fully autonomous vehicles will be navigating public roads, requiring (even more) robust cybersecurity countermeasures.

With the proliferation of CASE (connected, autonomous, shared, electric) technologies, the number of access points within a vehicle for cyberattacks grows. Reacting to and mitigating threats is of the utmost importance.

Cybersecurity in the automotive sector has its own unique challenges. For example, a vehicle's electrical/electronic (E/E) architecture is far more complex than a computer, and the average length of ownership creates longevity and update concerns.

The consequences of a vehicle being infiltrated by malware or targeted by hackers are much graver than for other consumer devices. This can result in loss of life and long-term reputational damage.

Research cited by the consultancy reveals the scale of the problem. As it notes, backend telematics servers are the most commonly hacked vector to take remote control of vehicles and exploit data, followed by remote keyless vehicle systems and third-party mobile apps in vehicles.

Other threat vectors include on-board diagnostic (OBD) ports, infotainment systems, sensors, electronic control and transmission control units (ECU/TCU), in-vehicle networks, Wi-Fi, Bluetooth, ODB dongles, cellular networks and USB ports.

As a result, Frost & Sullivan recommends automakers to use a multilayer solution to secure in-vehicle functions, the internal network, cloud-based apps and vehicle-to-data communications, and put in place incident response and mitigation plans to deal with potential breaches.

Trend #2: Expansion of the autonomous vehicle market

Autonomous vehicles set to account for 12% of car registrations by 2030

Autonomous vehicles (AV) are set to become a major transportation trend. Multiple IT and sensor technologies combined with electric drivetrains will bring about a driverless transport revolution.

- The first to be affected will be traditional delivery systems. These will rapidly be replaced, with electric delivery drones and vans becoming a familiar sight.
- AVs can also combat one of the major challenges of the trucking industry — a lack of drivers.

Advantages of AVs will include improvements to road safety, lower energy consumption, reduced congestion, easier commuting, and a reduction in the number of accidents caused by human error.

The World Health Organization estimates that every year the lives of approximately 1.3 million people are cut short as a result of a road traffic crash. Between 20 and 50 million more suffer non-fatal injuries, with many incurring a disability as a result of their injury.

The potential for AVs to reduce these numbers clearly has extremely far-reaching consequences.

60.1 million units

↗20.8% CAGR

anticipated global semi-autonomous vehicle market demand by 2028

AV road safety and cybersecurity are interdependent

Along with benefits of AVs come a number of risks concerning safety, legal liability, privacy and cybersecurity.

In 2021, early AVs were being constructed with 50–100 processors, each a potential target. Sensors in autonomous vehicles were also generating terabytes of data per hour.

Allied with the increasing number of cloud-based applications in the automotive industry, these technological advancements multiply attack surfaces and hence potential cybersecurity threats in the AV space.

The systems through which AVs receive instructions are also potentially vulnerable to cyber-hacking. Cyberattacks could target an individual AV, an entire AV fleet, or act as an entry point into any connected entity.

Plus, disrupting internet connectivity could wreak havoc — with serious road safety concerns, and the ability to cripple transportation by bringing thousands of private cars and commercial vehicles to a halt. Conventional vehicle maneuvers such as lane changing, parking, collision avoidance and braking could also be compromised, leading to serious accidents.

Securing against hacker attempts to take control of AVs

In future driverless vehicles (Levels 4 and 5), AI will do all the driving, and self-driving vehicles relying on multiple computers will inevitably expand the cybersecurity attack surface.

Key cybersecurity threats include assaults on the service components of autonomous systems, jamming of signals, or transmission of counterfeit information to other connected vehicles or their operators. Cybercriminals could take control of a vehicle through wireless networks such as Bluetooth, keyless entry systems, cellular or other connections as the car connects with the wider environment.

Over-The-Air (OTA) electronic communications that automatically upload data from self-driving cars also provide a huge opportunity for cyber intrusion, potentially affecting whole fleets of self-driving vehicles. And without sufficient security, Vehicle-to-Vehicle and Vehicle-to-Internet communication channels can be hacked. This leads to threats such as the injection of fake messages, compromise of global navigation satellite systems, using sensor manipulation to disorient the AV's systems, and ultrasound or radar interference to blind an AV from oncoming obstacles.

So while driverless vehicles are not currently a particularly profitable target for cybercriminals, as the technology develops and the number of AVs on the roads expands, they will become increasingly attractive — requiring manufacturers and cybersecurity experts to cooperate at each stage of AV development to design-in effective security.

Trend #3: Cybersecurity regulation in the transportation sector

Around the world, regulatory authorities are addressing the risks posed to the transportation industry by its vulnerability to cyberattacks.

In the United States, for example, the US Transportation Security Administration (TSA) has established a minimum set of cybersecurity requirements for rail and aviation operators.

- For **passenger and freight railroad carriers**, cybersecurity directives require a 24/7 cybersecurity coordinator, reports submitted to the Cybersecurity and Infrastructure Security Agency within 24 hours, cyber self-assessment and cyber incident response plans.
- TSA cyber requirements for **airports and aircraft operators** also include appointing a cybersecurity coordinator, immediate report of cyber incidents, and a cybersecurity self-assessment and cyber incident response plan.

In the automotive sector, cybersecurity regulations have intensified with the development of autonomous driving features such as electronic stability control (ESC) and automated lane keeping systems (ALKS).

In particular, the **United Nations WP.29 Cybersecurity regulations**, approved in June 2020, provide a framework for the automotive industry to implement processes to:

- Identify and manage cybersecurity risks in vehicle design
- Verify that risks are managed
- Ensure risk assessments are kept current
- Monitor attacks and respond to them
- Analyze successful or attempted attacks
- Review cybersecurity measures in the light of new threats
- Ensure security lifecycle management (across the development, production and post-production phases)

"With this (WP.29) directive, the UN is making automotive cyber security standards non-negotiable. The hope is that motorists will factor cyber security into their buying decisions — like air-con or heated seats."

UN Regulation No. 155 enforces these cybersecurity standards within United Nations Economic Commission for Europe (UNECE) member states, making them mandatory for all new vehicle types since July 2022, and for all new vehicles from July 2024.

Securing against fines and reputational damage

Identifying all possible vulnerabilities within a vehicle is essential, as is providing the associated mitigation procedures to follow in case of an attack — important prerequisites for complying with WP.29 and industry standards such as ISO 21434 and ISO 26262.

Breaching cybersecurity regulations means vehicle certification may be revoked. Moreover, the entire supply chain must comply with information security requirements. Car manufacturers accumulate vast amounts of data and must adhere to strict personal data regulations. Any breach of regulations can lead to massive financial penalties and damaging loss of reputation.

Manufacturers and operators of connected car fleets are also ultimately responsible for securing customers' data. Here too, regulatory fines and negative publicity following any data intrusion can lead to loss of market share and damage to the reputation of the company.

In 2021, for example, the operator of short-term car rental platform CityBee was fined €110,000 after an investigation by the Lithuanian data protection authority (VDAI) concluded the company's obligation to ensure the security of processing of personal data provided in the EU's General Data Protection Regulation (GDPR) was not met, and customers' personal data had been breached.

Trend #4: AI facilitates smarter route and delivery planning

Advanced technologies in transport and logistics

Artificial intelligence (AI) is unleashing the potential of big data in logistics and transport by enabling organizations to harness automation, robotics and advanced predictive analytics, optimize warehouse and supply chain management, and enhance customer experience.

However, in tandem with the huge gains from increasing efficiency and reducing costs, there is growing concern about the effects on cyber-resilience and driver and vehicle safety.

AI is particularly critical to the commercial transportation sector because the safe and timely movement of goods and cargo around the globe is a costly logistical challenge, for which AI creates numerous opportunities to reduce costs and improve operations.

Commonly adopted AI technologies include 'truck platooning' (which maintains an optimum speed and distance between trucks in a group, thereby reducing the overall time spent on the road), autonomous emergency braking (AEB), adaptive cruise control (ACC), collision warning, lane-keep assist, and advanced driver assistance systems (ADAS) to reduce driver fatigue and avoid potential road accidents, thereby saving lives and reducing delivery times.

Moving outside the vehicle, AI also underpins intelligent devices and real-time traffic management systems utilized to tackle the escalating global problem of traffic congestion.

$3.87 billion

↗15.8% CAGR

expected global artificial intelligence (AI) in transportation market size by 2026

AI in the skies

In the aerospace industry, AI-based virtual assistants are eliminating repetitive tasks in the air, and boosting pilot productivity and efficiency. AI systems are also scheduling required maintenance, reducing aircraft time not flying and enhancing safety. And airline companies are using AI to optimize flight bookings through analysis of weather patterns and historical passenger data, and streamline customer experience with facial recognition and self-service kiosks.

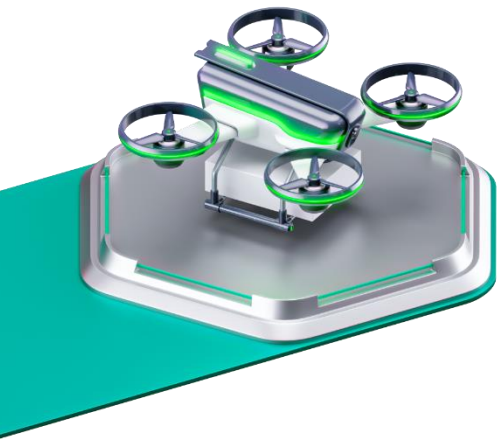
$16.23 billion
↗22.68% CAGR
expected global autonomous aircraft market size by 2027

Commercial autonomous flight is also just around the corner. Researchers at the University of Zurich, for example, have trained drones to fly autonomously at high speeds while navigating complex obstacles using onboard sensing and computation.

AI transformation in planning and delivery for shipping

AI is also a hot topic in the maritime world, where it can collect and analyze data enabling the container shipping industry to plan more accurately. Shipping industry majors such as Flexport, Maersk and Panalpina have initiated measures to harness AI to address an array of issues surrounding the industry.

Looking forward, a world-first journey of a zero-emission autonomous cargo ship took place in November 2021 between two Norwegian ports. All of the ship's movements were controlled from three onshore data control centers, and it is expected that robotics will eventually include unmanned loading and unloading, so the potential for the shipping industry is huge.



Last-mile transport by robots and drones

Another breaking trend in transportation technology is last-mile delivery robots. These usually take the form of unmanned ground vehicles and drones, which increase the speed of the last-mile delivery process, reduce the cost of delivery services for small and lightweight packages, simplify and reduce the cost of local transformation, eliminate delays, and can be fully integrated with software controlling the complete delivery process.

Securing against increased numbers of access points for cybercriminals

The increased use of fleet telematics systems using AI algorithms to track the location, status and condition of trucks creates more access points for hackers. For example, cyber-attackers could take over the digital dashboard of an AV carrying fresh produce and tamper with the temperature gauges or shut down the cooling mechanism, resulting in thousands of dollars' worth of spoilt food. The same applies to autonomous shipping and flights. Routes could be changed and transportation operations brought to a halt.

Occupants of AVs can also become so reliant on road safety technology that failures due to interference could result in serious accidents. As with all solutions combining high data content with sophisticated communications technology integrated with and connected to digital infrastructure, AI is vulnerable to cybercrime. Cyber-intrusion can transform drones and autonomous shipping into accidents waiting to happen or even lethal weapons.

Trend #5: Mobility as a Service (MaaS)

The global MaaS market is forecast to exceed $350 billion by 2025

On roads, on rail, at sea and in the air, operators are implementing ever more sophisticated systems to streamline the mobility of cargo and passengers. The new mantra is connected automation and technology as the enabler — in AVs, trucking fleets, airports, ports, railway systems, and distribution and logistics centers. Automation improves operational management, cuts costs by reducing labor requirements and helps smooth the overall customer experience.

As a leading example, Mobility as a Service (MaaS) is the future of the smart city — exemplified by highly convenient ride-hailing and ride-sharing platforms like Uber and Lyft, which are completely dependent on an increasingly digitally connected world.

MaaS combines public, private and shared transportation to move both people and freight. Easily installed software calculates the most efficient, cost-effective and speediest method of transport both for physical passengers and shipments — all of which is enabled by the combination of cloud-based platforms, smart analytics, network connectivity, total automation, blockchain technology and customer self-service models.

$ 888.97 million

↗ 49.93% CAGR

expected Global Blockchain Technology Market in Transportation and Logistics Industry growth during 2021-2025

- Cloud-based transportation management systems coordinate — in a single cloud-based platform — all the necessary information to facilitate each stage of every delivery. The software integrates all orders, customer data, route planning and client/customer communication, resulting in fewer costly errors and increased productivity.
- Predictive analytics enable better understanding of customer requirements and buying trends both now and in the future, so companies can plan more effectively. Combining vast quantities of data with smart analytics leads to reduced costs, less downtime and waste, better customer service (e.g. more on-time delivery) and identification of new patterns and business opportunities.
- Network connectivity is becoming the norm across all forms of transport. For example, 5G-connected cars will represent more than 90% of the market by 2028; the International Maritime Organization's (IMO) e-navigation program coordinates current worldwide data on the status of ocean shipping; and GSM-Railway (GSM-R, the Global System for Mobile Communications — Railway) is an international standard for wireless communications and applications linking trains to national control centers.
- Completing the picture, blockchain is an efficient, transparent system used to synchronize supply chains and track components, vehicle usage and maintenance history without the need for centralized control.

Between June of 2020 and June of 2021, the transportation industry witnessed a 186% increase in weekly ransomware attacks.

Securing against malicious system outages

With the proliferation of sensors, network technology and automation required for MaaS, the whole transportation industry will become an increasingly enticing target for cybercriminals and opportunists.

MaaS — connecting customers, data providers and transportation methods, as well as transferring huge volumes of data — is vulnerable to both cyberattack and data privacy issues. And cyberattacks on the transportation and logistics sector are already becoming more frequent

In June 2021, for example, the New York Times reported a cyber-hacking group had infiltrated computer systems of the New York Metropolitan Transportation Authority, a network used by millions of passengers each day. And in October 2021 a ransomware attack on Toronto's subway, bus and streetcar systems resulted in booking system and vehicle tracking problems, as well as data of 25,000 users being stolen.

Trend #6: Vehicle telematics goes granular

Speedier deliveries and more secure transport

In the transportation and logistics business, vehicle telematics technology extends much further than helping drivers find their destination. Today's solutions enable organizations to locate and track every movement of their products and personnel, improving planning and speed of delivery whilst minimizing costly errors.

Sophisticated telematics track metrics for entire fleets from each vehicle's 'black box', including vehicle speed, routes, fuel usage, driver behavior, engine start-up and shutdown, idling, engine load, temperature and condition.

Alerts inform if a vehicle is deviating from an assigned destination, the route taken and when the vehicle is resting. Advanced navigation informs drivers of optimal routes to avoid traffic congestion — speeding up deliveries. And vehicle telematics is a formidable tool for insurance companies in assessing accidents or locating stolen vehicles.

The IoT in the transportation market is expected to register a CAGR of 14.5% over the forecast period of 2021-2026

Telematic sensors also benefit public transport passengers, making route information available in real time, and providing rerouting features that enable people to plan alternative routes. Automatic transport management systems enable fast asset tracking, and physical assets can be tracked and managed online in real time. And smart city design incorporates Internet of Things (IoT) data on traffic and pedestrian management.

In the aerospace industry, telematics use is expanding exponentially because of the sheer amount of data generated by just one flight. A single-engine plane, for example, can reportedly generate more than 844TB of data in 12 hours.

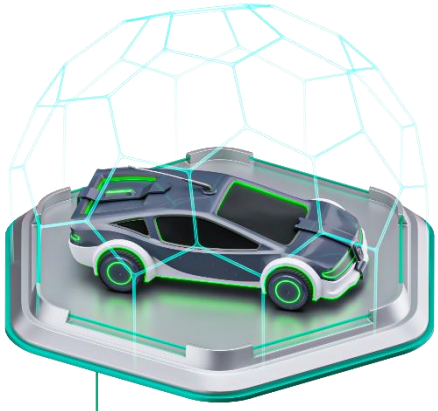
Telematics IoT connectivity is also being extensively used at every level of the maritime industry, from the individual components of a ship's engine room to cargo containers, fleet management and connected ports.

Securing against IoT cyberattacks

Because intelligent public transportation uses a combination of CCTV cameras, GPS devices, digital displays, automated stop announcements and Wi-Fi devices, cybersecurity is a must. When trains don't arrive or airports grind to a halt, the result is chaos that can affect many thousands of people.

GPS navigation and operational systems, for example, can be at risk of being insufficiently protected. In July 2020 Garmin, an international manufacturer of GPS products, was the victim of a cyberattack, and although the damage was relatively restricted, this served as a warning of the potentially disastrous consequences of future such attacks.

Transportation system telematics may also lack sufficient security processes. IoT devices brought rapidly to market may have insufficient built-in security, and personnel overseeing security may not be up to speed on latest IoT innovations being rolled out in their industry. If transportation supply chains are disrupted, the fleet operator, the end consumer, and ultimately whole sectors of the economy will suffer.



Partnerships hold the key to transportation security

With increasing digitization of key operational technology and human lives at stake, cyber-risks for the transportation industry have never been more acute. In automotive, for example, increasing attack surfaces mean cybersecurity will become too complex for OEMs to handle in-house, meaning they will require assistance from Tier 1 suppliers, automotive security and IT security companies.

As cybersecurity increases in depth, breadth and scope to tackle emerging threats, partnerships between these kinds of organizations will be crucial in establishing effective cybersecurity strategies; ensuring WP.29, ISO 21434 and ISO 26262 compliance; and creating end-to-end and tailored services such as vehicle security operations centers (VSOC) filling specific competency gaps.

Kaspersky is a pioneer in helping the transportation industry adopt optimum security strategies in today's volatile and challenging environment. Our tailored solutions and services, assisted by world-leading threat intelligence, protect data and business continuity 24/7 against advanced threats and targeted attacks — mitigating risks, detecting attacks earlier, dealing effectively with live attacks and fortifying future protection.

Our stage-by-stage cybersecurity approach is designed to clarify which level of security as well as which specific solutions suit your organization best. The frameworks provide a set of easily managed threat protection measures coordinating seamlessly with one another to meet the needs of each individual organization, and offer a cybersecurity roadmap assuring smooth transition from one IT security maturity level to another when the time comes.

We can also offer products and services specifically designed to provide cybersecurity for connected cars and their infrastructures, and support the development of new mobility technologies — including autonomous, electric and shared technologies — from IoT, ECUs and VSOC, to WP.29, ISO 21434 and ISO 26262 compliance.

Kaspersky's step-by-step cybersecurity approach

1

Kaspersky Security Foundations — essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to ...

2

Kaspersky Optimum Security — for organizations requiring more specialized security against new and evasive threats, before effortlessly implementing ...

3

Kaspersky Expert Security — for organizations with established mature IT security teams combatting the most complex targeted attacks.

kaspersky bring on the future

Cybersecurity maturity level	Solution
IT Smaller organizations without a specialized IT security team	**What** **Kaspersky Security Foundations** **How** Implement fundamental security for organizations of any size and infrastructure complexity delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. → **Endpoints:** Protect every endpoint in your organization with Kaspersky Endpoint Security for Business; Kaspersky Embedded System Security → **Cloud:** Benefit from borderless security with Kaspersky Hybrid Cloud Security → **Network:** Secure your perimeter with Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway → **Data:** Safeguard valuable and sensitive data with Kaspersky Security for Storage → **Security Management:** Access expertise with Kaspersky Premium Support; Kaspersky Professional Services
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** **Kaspersky Optimum Security** **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring — but without prohibitive costs or complexity → **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum → **Analysis and investigation:** Enhance threat visibility and simplified investigation process with Kaspersky Endpoint Detection and Response Optimum → **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with Kaspersky Endpoint Detection and Response Optimum and Kaspersky Managed Detection and Response Optimum → **Security awareness:** Equip employees with automated tools at all levels with cybersecurity skills with Kaspersky Security Awareness Training *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What

Kaspersky Expert Security

How

Complete mastery over the most complex and targeted cyberattacks

→ **Equipped**: Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. Kaspersky Anti Targeted Attack Platform with Kaspersky EDR at its core empowers your team with XDR capabilities.

→ **Informed:** : Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:

- Integrate actionable, immediate threat intelligence into your security program. Kaspersky Threat Intelligence gives you instant access to technical, tactical, operational and strategic threat Intelligence.
- Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with Kaspersky Cybersecurity Training.

→ **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:

- Take advantage of immediate support from the Kaspersky Incident Response team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
- Bring in a second opinion and managed threat hunting expertise from a trusted partner with Kaspersky Managed Detection and Response, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
- Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through Kaspersky Security Assessment.

kaspersky bring on the future

Targeted Solutions

What	How
 **Kaspersky Embedded Systems Security**	A multi-layered solution delivering unequalled protection to Windows- and Linux –based embedded devices — even those with limited system resources and running older software. Offering a solid basis of system hardening technology stack, it adds multiple opt-in security layers such as exploit prevention or anti-malware, which means protection can be optimized for devices of different power levels— including vulnerable discontinued devices and PCs running unsupported Windows OSs such as Windows XP.
 **Kaspersky Security for ECUs**	A software solution to be installed on automotive electronic control units (ECUs). It provides control mechanisms and real-time intrusion detection for connected vehicles, their internal and external communications, as well as for 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 meet compliance and continuous monitoring requirements.
 **Kaspersky Threat Attribution Engine**	A malware analysis tool deployed on your network, “on premise”, or Amazon Web Services (AWS) that incorporates 27 years of Kaspersky’s database of APT malware samples. Delivers automated analysis of the “genetics” and “genotypes” of malware for code similarity with previously investigated APT samples to rapidly link new attacks to known APT malware, actors, campaigns and previous targeted attacks.
 **Kaspersky Research Sandbox**	Emulates company-specific systems in an isolated environment, performing automated, behavioral malware analysis and enabling safe detonation, and detection of advanced and previously unseen threats.

Cyberthreats News: www.securelist.com

IT Security News: www.kaspersky.com/blog

Threat Intelligence Portal: opentip.kaspersky.com

Technologies at a glance: www.kaspersky.com/TechnoWiki

Awards and recognitions: media.kaspersky.com/en/awards

Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky bring on the future