

WHITEPAPER

Security turbo: What helps the automotive industry in the fight against cyber threats

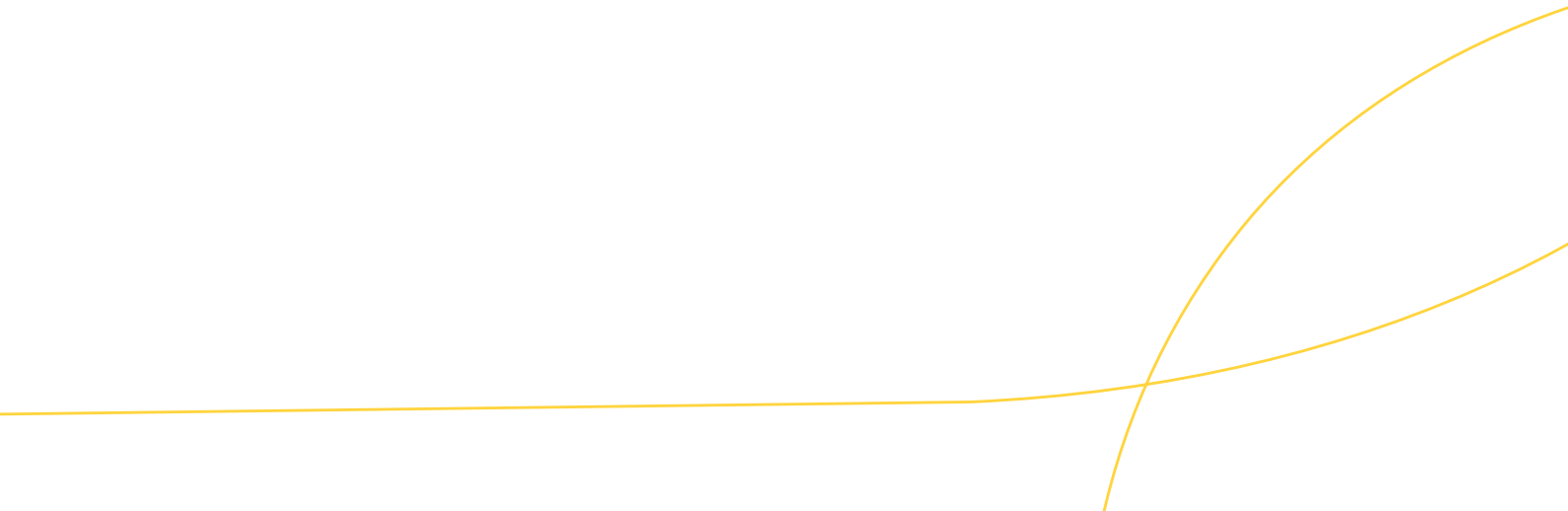


Security turbo: What helps the automotive industry in the fight against cyber threats

The automotive industry, once a bastion of mechanical engineering, is now at the forefront of the digital revolution, driven by increasing networking and the emergence of new technologies. The transition from mechanical to digitally networked systems brings with it new challenges in the area of cybersecurity and data protection. Vehicles are no longer primarily at risk from physical theft, but from digital attacks.

In the 1970s, cars were essentially mechanical constructions that were hardly influenced by what is now known as digital technology. At that time, physical theft was considered the main problem: burglars used techniques such as breaking open door locks or bypassing the ignition so that they could start the car without the key. In addition to the use of false keys, violent robberies were also a threat. With the advent of digital technologies in the 1980s and 1990s, the security risk changed: vehicles became networked systems that offered new targets for hackers. The threat of cyberattacks increased.

In the 2000s, cyberattacks by hackers came to the forefront, but were not yet as developed, industrialized, and professionalized. Security risks in connection with digital attacks were becoming apparent, but were still in their infancy. The 2010s brought another change: keyless entry systems and networked infotainment and telematics systems became standard. The interception of radio signals and the possibility of remote access to vehicles turned out to be new security risks. Today, in the 2020s, the automotive industry is once again undergoing a rapid technological transformation, spearheaded by connected car technologies and software-defined vehicles (SDV). These innovations are not only changing the way cars are developed and used, but are also presenting developers with new challenges in the area of cybersecurity.



Why a comprehensive security strategy is necessary

Imagine a world where hackers can take control of your vehicle by manipulating brakes, steering, and even engine performance. This is not distant science fiction, but a real threat that has serious consequences for passenger safety and significant economic damage for car manufacturers and the entire industry. In the hidden corners of the digital world, where invisible technology networks permeate our everyday lives, a seemingly inconspicuous element like a car's tail light becomes a critical access point. It opens the door to the vehicle's Controller Area Network (CAN bus), which can jeopardize the entire vehicle functionality if misused.

In this increasingly network-connected world, the attack vectors are diverse and complex. Potential gateways for such attacks include not only obvious interfaces such as Bluetooth and Wi-Fi, but also less noticed points such as on-board diagnostic ports and even vehicle firmware updates. Once in the system, hackers can exploit vulnerabilities in the software to send control commands to various vehicle components. Such attack patterns range from simple malfunctions (such as the unexpected activation of the windshield wiper) to deep interventions in the vehicle control system.

The complexity of attacks on cars varies greatly and manifests itself in different aspects. On the one hand, some attacks can be carried out remotely and automatically, without physical access to the vehicle. On the other hand, there are scenarios that require physical access to compromise the car. These differences in design show the range of threats to which automobiles can be exposed. In addition, attacks are concentrated on both individual vehicles and entire vehicle fleets. This points to the need not only to secure individual vehicles, but also to protect the entire fleet infrastructure from potential threats.



The location of the attack also plays an important role, which can be varied and extend over different phases of vehicle use and manufacturing. Attacks can take place in the workshop during maintenance by exploiting security gaps in diagnostic software or hardware. However, they can also take place during the production phase at the manufacturer by intervening in the production process or in software development. Attacks are even possible at the level of subcomponents such as chips or other critical components.

Holistic approach

In view of these risks, it is crucial that all players along the value chain — from car manufacturers and suppliers to software developers — develop a deep understanding of potential security vulnerabilities. You must take proactive measures to minimize these risks. A holistic approach therefore requires close cooperation between all parties involved in order to implement and continuously maintain uniform security standards and protocols along the entire chain.

The focus here is on implementing a holistic security strategy that encompasses both the hardware and software levels. This strategy should be flexible enough to adapt to constantly changing cyber threats. This includes regular safety checks, updating protective measures, and continuous training of employees to increase safety awareness and safety skills. In addition, it is important to develop and implement robust emergency response plans in the event of a successful cyberattack. The focus is on quickly identifying and eliminating security vulnerabilities and minimizing potential damage. If every participant in the value chain accepts their responsibility and acts proactively, this ensures a high level of security and trust in the increasingly networked and digitalized automotive industry.



Organizational compliance

In order to meet the complex requirements for vehicle safety, it is essential to ensure both organizational and regulatory compliance. At an organizational level, this includes compliance with internal and external regulations, standards and best practices that are of particular relevance to automotive cybersecurity. The focus is on ensuring that both automotive manufacturers and suppliers meet the legal requirements for data protection and data security and at the same time comply with best practices and guidelines such as ISO 27001 or IEC 62443. These standards minimize the security risks in networked vehicles.

Establishing a comprehensive compliance program also promotes a culture of cybersecurity, raises employee awareness, and reduces the risk of human error. Regular audits and reviews help the auto industry comply with security guidelines and adapt to new threats. It is important to include suppliers and partners in the compliance strategies in order to ensure uniform safety standards along the entire value chain. This strengthens customer confidence and contributes to the success of the industry.

Regulatory compliance

Regulatory compliance focuses in particular on compliance with the legal requirements for the safety of connected vehicles. Here, the UNECE (United Nations Economic Commission for Europe) plays a central role in setting global standards, with UN Regulation No. 155 defining the safety requirements for autonomous vehicles. The EU directive on cybersecurity in the automotive sector supplements these standards and ensures that vehicles sold in the EU meet the necessary security requirements.



These international and regional regulations protect public safety and facilitate international trade in vehicles. Regular security assessments and audits ensure compliance with current security standards, promote consumer confidence, and support the development of innovative, secure automotive cybersecurity solutions.

Important standards and regulations

ISO 27001

ISO 27001 is a standard for information security management that defines requirements and best practices. In the automotive industry, it protects sensitive information and meets high standards.

IEC 62443

IEC 62443 is an international series of standards for industrial network security that defines standards and guidelines for the protection of automation systems and industrial control systems (ICS).

UNECE/ UN Regulation No. 155

The UNECE (United Nations Economic Commission for Europe) develops international standards for vehicles and road safety. UN Regulation No. 155 deals with safety requirements for autonomous vehicles.

Smooth cooperation in the automotive value chain

The complex value chain in the automotive industry requires smooth cooperation. This requires precise coordination and efficient communication between all parties involved — from original equipment manufacturers and suppliers to all players in the automotive aftermarket (spare parts market including dealers and workshops). The integration of security standards from the outset, regular security checks, and targeted training to raise awareness of security risks play a central role in this structure. Only strict adherence to applicable compliance rules and standards guarantees a comprehensive cybersecurity strategy.

The importance of investing in cybersecurity within a value chain cannot be overestimated. Such investments not only have a direct impact on the company itself, but also affect all players in the chain. The concept of the "weak link in the chain" makes it clear that the stability of a value chain is only as strong as its weakest link. Investment in cyber defense acts as a strong line of defense, while lack of investment weakens this line. If a company neglects cybersecurity in the value chain, attackers can exploit precisely this vulnerability to attack the entire chain.

This also increases the costs and risks for all other companies. This is why a holistic view of cybersecurity along the value chain plays a central role in keeping vehicles safe from attacks.

The automotive ecosystem is made up of numerous players: car manufacturers, suppliers, service providers, regulators, and end users. Car manufacturers are responsible for vehicle development and the integration of technologies, while suppliers provide the necessary components right through to the workshop. Service providers offer comprehensive networking and software solutions. Regulatory authorities set standards and laws, while end users move the vehicles.

In the context of cybersecurity, the value chain comprises various elements, including cybersecurity stacks consisting of hardware, software, services, unified threat management, vulnerability management, application security, managed security services, and risk and compliance. The integration and effective coordination of these elements provides comprehensive protection against cybersecurity threats and helps to secure the entire automotive ecosystem.

Which recommendations for action and approaches make sense

Cybersecurity requirements are becoming increasingly stringent in the rapidly developing automotive industry. Vehicles are changing from a means of transportation to a part of our digital lives, making the protection of data and systems more important. Successful companies need a dynamic cybersecurity strategy that includes technical innovation and continuous training. Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) are regarded as key players in this process. Their task is to harmonize technological progress and data security and to promote industry-wide cooperation in the development of common security standards. Here are some selected recommendations.

1) V2X communication technologies: innovations and their protection

Important for car manufacturers: They must ensure that V2X systems (V2X: Vehicle-to-Everything communication) are resistant to cyber attacks while maintaining data protection and security.

Example & recommendation: An OEM (Original Equipment Manufacturer) integrates end-to-end encryption into the V2X communication of its vehicles. CISOs should conduct regular penetration tests and security assessments to identify and address vulnerabilities before launch.

2) Multi-layered security approach: multi-layered defense strategies

Important for suppliers: Develop a multi-layered security concept that includes various lines of defense.

Example & recommendation: A supplier of vehicle parts uses intrusion detection systems and regular security updates. CISOs should develop a framework for incident response and recovery plans in order to be able to react quickly to security incidents.

3) Security and data protection challenges in production

Important for manufacturing companies: Implement effective data protection and security measures in the production chain.

Example & recommendation: A manufacturer of vehicle components conducts security training for employees and uses secure cloud technologies to store sensitive data. CISOs should conduct regular audits to verify compliance with data protection guidelines.

4) OTA updates: security in software maintenance

Important for software developers in the automotive industry: Ensure that OTA software updates (OTA: Over The Air) run securely and reliably.

Example & recommendation: A software supplier for connected vehicles implements multi-level authentication procedures for OTA updates. CIOs should invest in robust monitoring systems to ensure the integrity of the software throughout the update process.

5) SASE and Zero Trust models: advanced security concepts

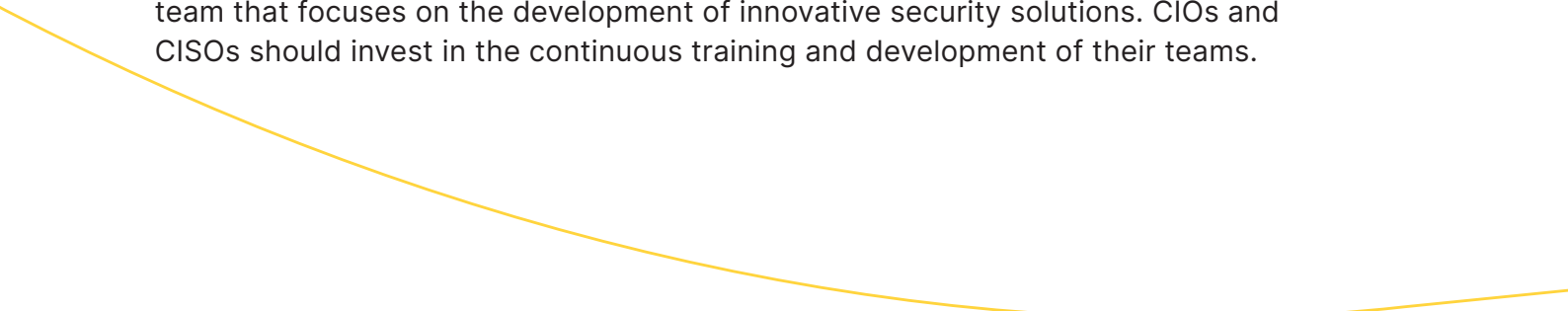
Essential for IT departments in the automotive industry: Introduce dynamic access controls and comprehensive verification of every connection.

Example & recommendation: A vehicle manufacturer implements Zero Trust security models for access to the internal network. CISOs should ensure constant monitoring and dynamic adaptation of security policies.

6) The role of IT and security experts: proactive risk mitigation

Important for IT and security teams: Automotive companies should build a competent team to continuously adapt to new threats.

Example & recommendation: An automotive supplier establishes a cybersecurity team that focuses on the development of innovative security solutions. CIOs and CISOs should invest in the continuous training and development of their teams.



7) Integration of cybersecurity into the supply chain

Important for the entire value chain: Anchor security awareness in all areas of the supply chain.

Example & recommendation: A logistics company for automotive components implements stricter security protocols for data exchange between suppliers and manufacturers. CISOs should encourage security audits along the entire supply chain to identify and remediate vulnerabilities.

8) Compliance and adherence to data protection laws

Action required by international automotive companies: Ensure compliance with global data protection laws and standards.

Example & recommendation: A multinational automotive group regularly adapts its data protection strategies to international standards. CISOs should establish a dedicated team to monitor compliance with data protection laws.

9) Partnerships for joint security initiatives

Important for small suppliers and start-ups: Establish collaborations with larger companies to develop common safety standards.

Example & recommendation: A start-up in the field of autonomous driving works closely with established OEMs, which helps in the development of safety protocols. CIOs and CISOs should utilize the knowledge and resources of large partners to drive security initiatives forward together.



What Cloudflare can do for the automotive industry in the area of network security and data protection

As a leading provider of network security and cybersecurity, Cloudflare has established itself as an indispensable partner to the connected automotive industry. With its advanced technology and extensive experience, Cloudflare offers customized solutions that optimize online presence and network efficiency and security for businesses in this industry. These solutions play a decisive role in an increasingly networked world in which the demands on the performance and security of systems are constantly increasing.

But what does this mean for the suppliers who are responsible for the production and delivery of vehicle components? For them, integration into the Cloudflare network is invaluable. With solutions such as Firewall-as-a-Service, Cloudflare ensures that communication and data exchange between suppliers and manufacturers is secure and reliable. This guarantees efficiency and security throughout the entire supply chain.

Car dealers and garages also face the challenge of connecting securely to manufacturers' central systems. Cloudflare enables you to do this safely and efficiently. Such network services play a central role, particularly for the secure receipt and implementation of over-the-air updates. And the end users? Although they do not interact directly with Cloudflare, they benefit indirectly from the enhanced security and network services that Cloudflare provides to OEMs and suppliers. A more secure and efficient network leads to a better user experience and more reliable services.

Cloudflare offers a platform that supports the needs of all players in the automotive industry. From optimizing online presence to improving network efficiency and ensuring security, Cloudflare optimizes the performance and security of systems in the connected automotive industry.

Conclusion

It is crucial for managers in the automotive industry to continuously adapt to the challenges of cybersecurity. With the increasing importance of connected vehicles, they must increasingly rely on innovative security mechanisms and robust data protection measures. The combination of advanced technology, regular employee training, and teamwork is at the heart of developing effective security strategies. The selection of a leading, expert, and visionary service provider is essential. By constantly adapting to new threat landscapes and complying with international data protection standards, managers can not only increase security, but also strengthen competitiveness and secure customer trust.

About Cloudflare

Cloudflare, Inc. (NYSE: NET) is the leading provider in connectivity cloud. As an enterprise, Cloudflare empowers organizations to make their people, applications, and networks faster and more secure everywhere, while reducing complexity and cost. Built on one of the largest and best-connected networks in the world, Cloudflare blocks billions of online threats for its customers every day.

Contact address:

County Hall/The Riverside Building,
Belvedere Road
London, SE1 7PB

Contact:

Telephone: +44 20 3514 697
Email: enterprise@cloudflare.com
<https://www.cloudflare.com>



© 2024 Cloudflare, Inc. All rights reserved.
The Cloudflare logo is a trademark of Cloudflare.
All other company and product names may be
trademarks of their respective companies.