Kaspersky Automotive Adaptive Platform β*

Solution for smart car manufacturers and ECU developers. Let Kaspersky take care of the cybersecurity so that you can focus on the product functionality

Key benefits

- Automotive grade
- Secure by design
- Multi-layer cybersecurity system
- Modular and flexible
- Compliance

Multi-layer security system
Protection at several levels:

Device level

- Device software/firmware alteration
- Downgrade/rollback attacks

Communication level

- Man-in-the-middle attacks/ session hijacking for:
  - Message spoofing, code injection, replay attacks
  - Interception of information/ monitoring communications
- DoS attacks on CAN bus
- Malicious diagnostic sessions (CAN-TP)

Application level

- Supply chain attacks (compromise of third-party components)
- Malicious code execution (exploits, malware)
- Corrupted applications

Security by default

Software development for electronic control units based on KasperskyOS cybersecurity technologies. Anything not specified in the security policies is prohibited by default. Even if a component proves vulnerable and comes under attack, it cannot affect the performance of critical system functions.

Compliance with standards

Kaspersky Automotive Adaptive Platform and the applications based on it meet the AUTOSAR Adaptive standard. Furthermore, the platform also complies with international regulatory frameworks for safety and cybersecurity.

Comprehensive approach

Software developed with Kaspersky Automotive Adaptive Platform facilitates the development of a comprehensive ecosystem of applications for embedded vehicle systems. This approach ensures system reliability and functionality at each level.

Compatibility

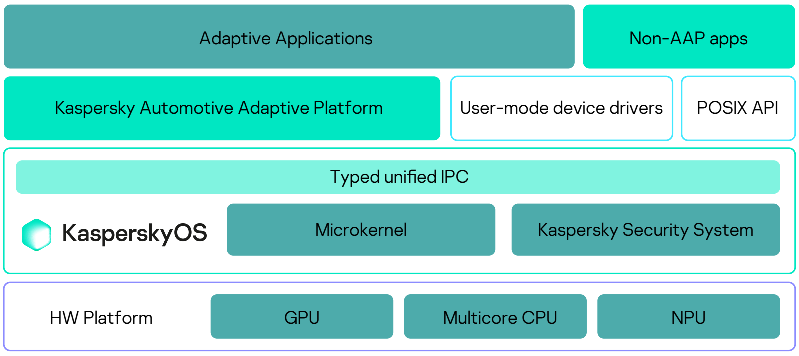
Applications built on Kaspersky Automotive Adaptive Platform can be used in high-performance controllers in mixed-criticality scenarios.

Flexibility and convenience

Support for multicore architecture and easy prototyping. Integration with vehicle security operations centers (VSOCs) should have been done during H1 2023.

Service-oriented architecture

Electronic assembly-agnostic development: ability to run adaptive applications and transfer non-AUTOSAR services to the platform without compromising performance or security.



Elements comprising the Kaspersky Automotive Adaptive Platform solution

* Ready for prototyping

Protecting connected ECUs

- DCU
- TCU
- HAD / ADAS
- HPC

Key features

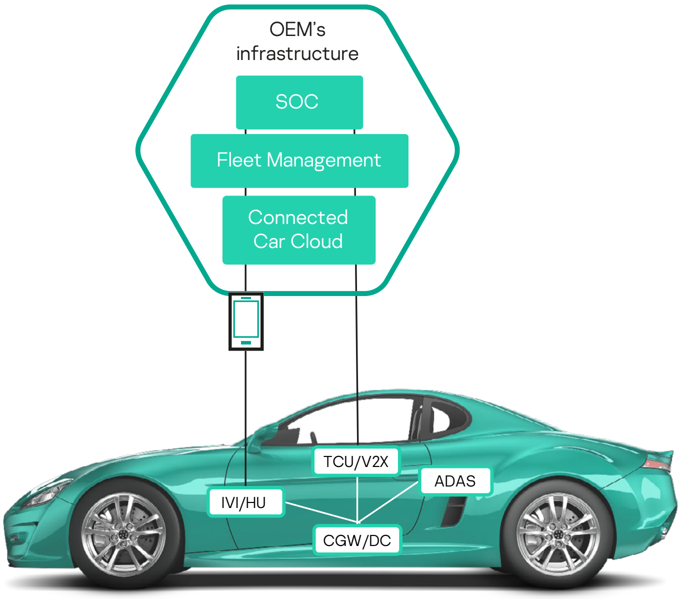
- Service-oriented architecture
- Designed for easy reuse across ECUs
- OTA
- Strong isolation of components
- Tailored cybersecurity controls

Covering multiple attack scenarios

- Zero-day exploits
- Supply-chain attacks/malware
- MiTM attacks
- Attacks via automotive bus
- Rollback/firmware alteration

Multilayer protection for various attack phases (initial access, privilege escalation, lateral movement, etc.)

Connected cars are not just vehicles with integrated digital systems – they have become smart infrastructures with mobile management apps, OEM clouds, fleet management systems, and more. As a result, the internal ecosystems of connected cars have multiple entry points vulnerable to cyberattacks.



Vehicle connectivity and ecosystem

Why Kaspersky

- Strong player and innovation leader in cybersecurity
- Automotive grade cybersecurity approach
- End to end solution provider
- Cybersecurity protection beyond current standards
- Partnership with industry leaders
- Experienced team of experts
- Holistic approach to ecosystem protection

More information about Kaspersky Cyber Immunity is available at **os.kaspersky.com**

kaspersky