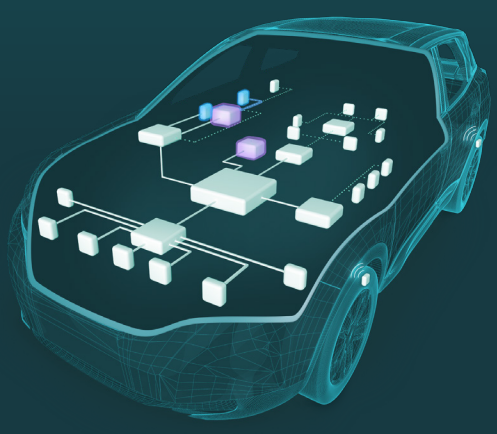
Explore How Our Products Secure Vehicles

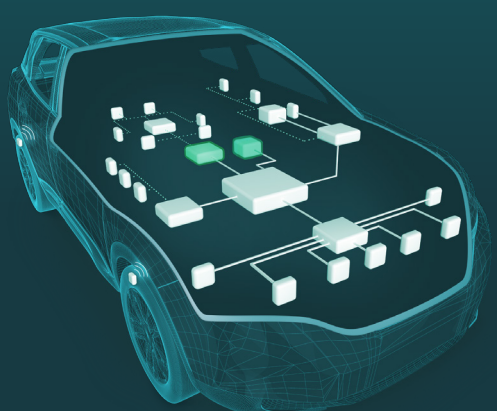
C2A'S EMBEDDED CYBERSECURITY APPLICATIONS FOR THE CONNECTED VEHICLE

PERIMETER NETWORK

Perimeter devices and the CAN bus connecting them are considered to be weakest spots in the vehicle.
C2A Fortifies these components using a unique decentralized firewall, that adds a security layer for CAN bus, with enhanced network IDPS capabilities.

*C2A - NXP Joint solution: Iron-Clad perimeter protection enables automotive manufacturers to provide a comprehensive protection from CAN bus cyberattacks.



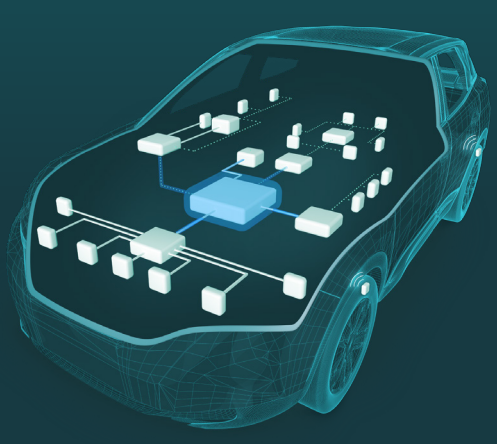


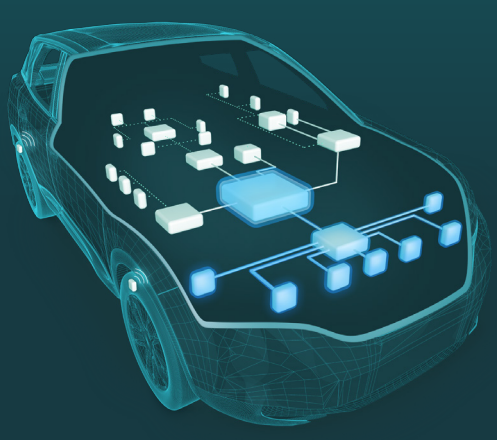
TCU / HEAD UNIT

The TCU and the Head unit are responsible for the rich and connected driver experience but at the same time they might be compromised by a remote attacker.
C2A's Endpoint Protection keeps in-vehicle ECUs safeguarded, by offering comprehensive runtime detection and prevention of attacks while in progress.

CENTRAL GATEWAY

The Central Gateway is the vehicle's backbone: It is the gate for all data coming into the vehicle, and responsible to route all in-vehicle communication in a safe and secure manner.
C2A protects the vehicle networks by detecting and mitigating real-time cyber-attacks on the CAN, CAN FD, LIN, Ethernet and FlexRay networks, with cross-network analysis capabilities. C2A's Network protection is suitable for current and future vehicle architectures.





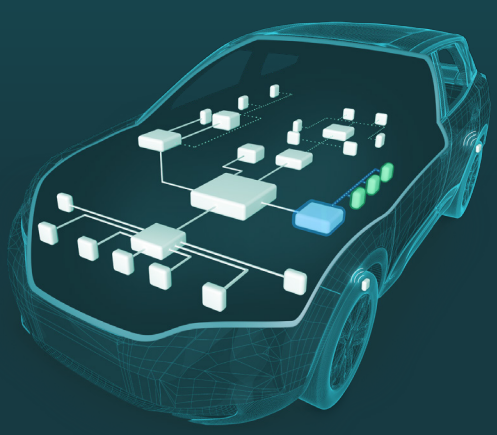
ADAS SYSTEM

ADAS systems are designed to automate and enhance the driving process in the pursuit of safety and better driving experience. However these systems expose new safety-critical attack surfaces.
C2A protects ADAS Systems with its Ethernet network IDPS. The solution includes a structured process for the configuration and generation of automotive IDPS.

*C2A's Automotive Grade Ethernet Firewall solution is integrated with NXP's and Marvell's new automotive Ethernet switchs.

POWERTRAIN

The powertrain are the actual components that make the vehicle go – the engine and the transmission. Cyber Attacks focused on these components could halt the vehicle while travelling at speed or cause false data to be sent to other safety critical ECUs within the vehicle.
C2A protects these crucial components combining its network IDPS capabilities and its Endpoint protection that supports safety ECUs, preventing damage to the vehicle and its occupants



* C2A Adds an Additional Security Control to Vector's AUTOSAR Basic Software. This integration – the first of its kind – enables developers to add an additional security control to automotive ECU projects without impacting time to market or harming safety compliance, and with a negligible runtime performance impact.