ENABLING **INSURANCE FOR FLEETS**

Automotive Cybersecurity Solutions that **Enable Insurance Companies And Aftermarket Vendors** to Implement State of the Art **Cybersecurity Protection** for Vehicles and Fleets

FLEET PROTECTION IN THE FACE OF VEHICLE HACKING

Car manufacturers want to know how each of their cars is behaving. 100+ embedded electronic control units (ECU) and several secure data stores are recording performance, usage and other data in real-time and periodically uploading gigabytes to the manufacturer's data center for analysis.

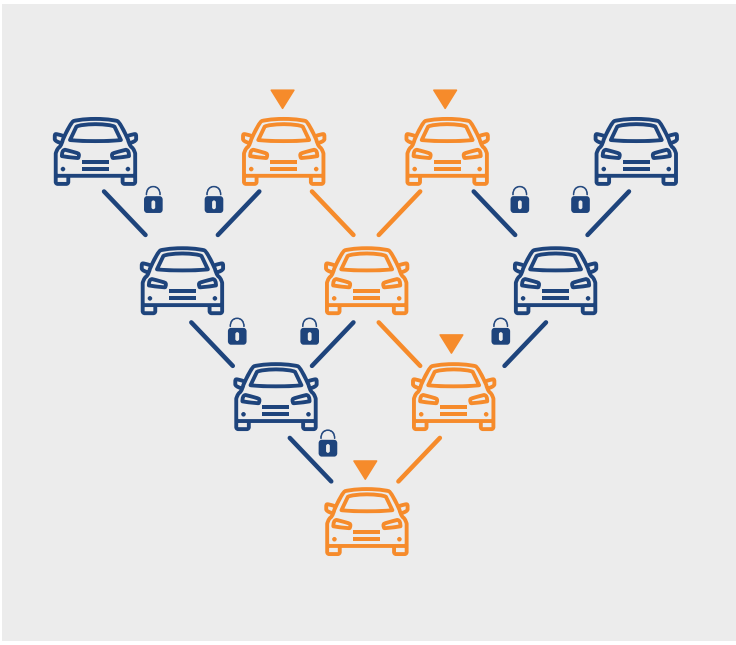
Fleets and Fleet Management Systems are highly connected and require robust cybersecurity for fleet cyber health as every vehicle is an endpoint and potential revenue generator. It is imperative to implement the most stringent and deterministic protection for predictive maintenance, reporting, retention, data flow and more.

CYBERSECURITY AND THE FLEET

Advanced fleet management relies on the constant flow of accurate data directly from the vehicles to the fleet manager's data center. In order to ensure the highest level of security and protection against malicious hacking attempts, data must be secured both at rest within the vehicle and while in transit from the vehicle to operational databases.

SUCCESSFUL VEHICLE HACKING ATTACKS COULD RESULT IN:

- Costly ransomware injections
- Loss of command and control communication with vehicles
- Extensive cost and adverse effects of loss of cargo
- Interruption in incoming data from or to vehicles
- Inability to access location data and services for route planning
- Infiltration and exfiltration of data
- Inability to send over-the-air (OTA) updates to vehicles

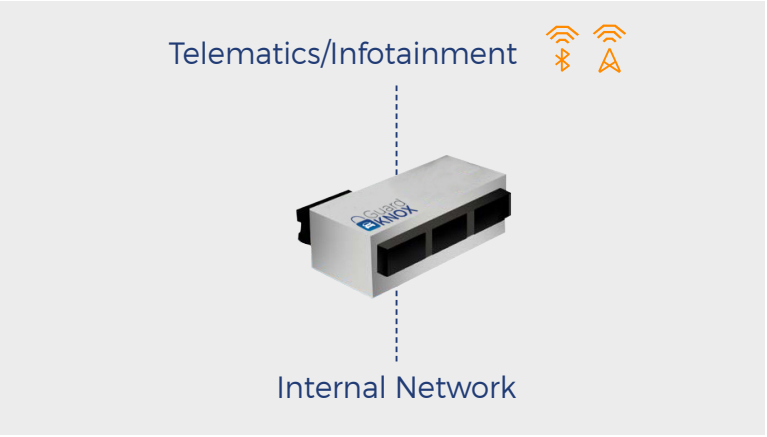


All data, at rest or in transit, needs to be periodically uploaded. As the accumulation of telemetry and other data increases, it must be secured with the highest level of confidentiality, integrity and availability. Deletion of data could have potentially devastating consequences.

ENABLING **INSURANCE FOR FLEETS**

LOCAL SECURE NETWORK ORCHESTRATOR (SNO™) SEAMLESSLY RETROFITTED AS A SIMPLE PLUG-IN

GuardKnox's unique value proposition brings solutions to the automotive industry that provide a secure end-point for high performance data hosting, processing, storage and filtering which also support secure cloud communication, data AI and analytics.



The joint collaboration between GuardKnox and Palo Alto Networks enables true end-to-end solution and protection. By using Palo Alto Networks expertise in network and cloud security with GuardKnox's expertise in automotive security and innovative technology. Manufacturers can secure OTA communications between the vehicle, the cloud and their operational centers.

The SNO™ is an especially attractive aftermarket solution, fitting seamlessly into the automotive value chain without requiring any third-party integration. The SNO™ is a simple plug-in that can easily be installed in the OBD port during vehicle manufacturing or retroactively in the aftermarket.

INCENTIVIZED POLICIES FOR INSURANCE PROVIDERS

Connected cars provide insurance companies with tremendous opportunities as new types of data may permit the construction of new types of insurance plans.

But, when it comes to specifying and pricing cyber insurance for connected vehicle owners, and especially fleet operators, insurance companies historically have not had the capability to determine if the fleet is adequately protected against ransomware and other cyber-attacks.

Insurance providers can offer incentivized policies under the condition of installation of the GuardKnox SNO™ - not only prohibiting access to entire fleet by way of infiltration of one vehicle, but also potentially tapping into new markets and creating additional revenue streams for insurance agencies.

USE CASES:

- **Secure Telematics ECU (TGU):** Ensure both the secure functioning from any external cyber threats as well as securing the data obtained from the device
- **Ransomware Protection:** Create the secure in-vehicle environment to ensure no vulnerability is exploited or used as a stepping stone to take control of any vehicle in the fleet to protect not only data, but more importantly, cargo
- **Secure Fleet Management Protection:** Guarantee that any improper command or communication to any ECU is ignored and immediately reported to maintain fleet integrity