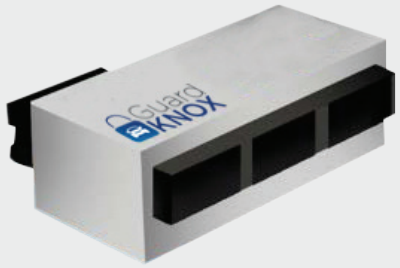
# GUARDKNOX **SECURE NETWORK ORCHESTRATOR™ (SNO)** SOLUTION


- Comprehensive robust automotive cybersecurity solution as the platform for added connectivity, safety, services, OTA updates and vehicle customization
- Localized and external protection for a single network (ECU)
- High performance, flexible, scalable, future-proof protection designed for integration by OEMs and aftermarket providers
- Patented Communication Lockdown™ methodology for multi-layer protection against all types of known and unknown cyber attacks
- Patented Service Oriented Architecture (SOA) - allows unified communication as well as access control and service level partitioning to secure further levels of connectivity, customization, and additional revenue streams across the automotive value chain
- Ability and flexibility to provide complete solution (including all HW/SW requirements) design per OEM's and/or Tier 1's specification – including secure EV ECUs

## A COMPREHENSIVE VEHICLE CYBERSECURITY SOLUTION:
## THE FOUNDATION FOR CONNECTIVITY AND CUSTOMIZATION

*As vehicle complexity and connectivity requirements increase, the need for post-production scalability and extensibility is rising. Furthermore, a secured end-point within the vehicle becomes increasingly vital to the automotive value chain as well*



The External-Local SNO™ Controller locks down and secures a single ECU with external connectivity.

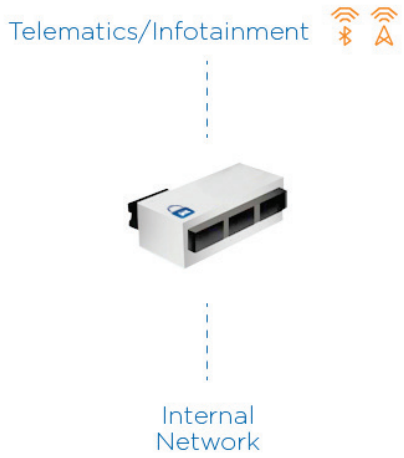
GuardKnox's Secure Network Orchestrator™ (SNO) product lines offers comprehensive vehicle cybersecurity protection against any type of known and unknown cyberattack. With a full software stack and hardware architecture, GuardKnox's patented technologies adhere to the most stringent security (ISO 15408) and safety (ISO 26262) standards. SNO™ solutions comply with GDPR (General Data Protection Regulation) and provide holistic automotive cybersecurity that easily fits the automotive tiered value chain while alleviating the difficulties of software only integration.

The GuardKnox External-Local SNO™ Controller is the only single network (ECU) solution that adjusts to end-users wants and needs as they evolve over the vehicle life span.

## VEHICLE-WIDE AND LOCALIZED, SINGLE INTERFACE (ECU) PROTECTION

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

GuardKnox's External-Local SNO™ Controller allows the automotive industry to add robust security to a single network in a cost-effective manner. The External-Local SNO™ has a flexible configuration and enough spare resources (computing power, internal memory, external I/O interfaces) to support additional levels of connectivity, such as personalized application downloads, provided by OEMs and Tiers 1s – supporting end-users trends of increased data consumption.




The GuardKnox External-Local SNO™ can be connected to any single ECU with external connectivity while simultaneously providing extensive connectivity protection. Ideal for telematics, infotainment, OBD, fleet management systems and other externally connected ECUs, it is integrated during production of the ECU or is installed or retrofitted by Tier 1s as an extension between the ECU and the rest of the vehicle. The External-Local SNO™ can be implemented in passenger cars, vans, trucks, fleets and more.

## FLEXIBLE, SCALABLE FUTURE-PROOF PROTECTION

The GuardKnox External-Local SNO™ cybersecurity solution has a flexible configuration built around a multi-core CPU and an FPGA module with extensive embedded capabilities. The solution's flexible configuration enables OEMs to incorporate only the required GuardKnox security functionality into their vehicle design, such as a specific number and type of vehicular bus interfaces or specific types of encryption engines, etc.

If additional security capabilities are required at a later date, such as additional bus interfaces, interface types, or additional types of encryption capabilities, etc., the OEM can activate the spare capacity in the existing FPGA of the Secure Network Orchestrator™ device without changing the footprint of the SNO™ or the BOM of the vehicle, resulting in extensive cost reductions.

## PATENTED COMMUNICATION LOCKDOWN™ ARCHITECTURE

GuardKnox's patented three-layer Communication Lockdown™ architecture enforces an ongoing, formally verified, and deterministic configuration of communication among the multiple bus networks embedded in the vehicle.

This approach allows unified communications as well as customizable access control and service level partitioning for all internal and external vehicle communications.

**The three layers of Communication Lockdown™ architecture are:**

### Routing Layer

The routing layer creates a physical separation between different networks using the FPGA and enables the GuardKnox SNO™ to differentiate messages by their origin. For example, if a message from the ECU of the right mirror tries to go to the ECU of power train, it will be discarded and reported.

### Content Layer

The content layer is used to lock all bits in each field of all messages for the entire vehicle. GuardKnox uses the CAN dB file as a source map for the bit in each message and populates open fields or bits with values that are agreed upon with the OEM. If a hacker has changed one bit in the content layer, the message will be discarded and reported.

### Contextual Layer

The content layer is used to create a state machine topped by a configuration file (a communication schema) that is build out of the two documents mentioned above. This state machine compares and enforce the real performance of the vehicle in the real world to what the network is doing or thinks it is doing.

## PATENTED SERVICES-ORIENTED ARCHITECTURE (SOA)

GuardKnox's patented Service Oriented Architecture enables additional levels of connectivity and customization through access control and service level partitioning to maintain vehicle integrity while increasing end user personalization. GuardKnox's already patented Communication Lockdown™ Methodology enables a multi-platform and multi-service approach with the ability to host multiple operating systems and services on one ECU with secure separation and full permission control. SOA has a secure separation (both hardware and software) between all resources, application groups, and operating systems, simplifying edge computing capabilities by providing ample processing resources with maximal flexibility both in interface support and provision for future software extensions/additional service being added.

**GuardKnox SOA patented technology creates the secure environment which enables added services and applications by hosting downloads or upgrades on the SNO™ platform throughout the lifecycle of the vehicle.**


This enables mission critical and non-mission critical applications to run simultaneously without interference; if one application should be compromised, all others will not be affected. This in essence converts the driver of a vehicle to a subscriber of features and functions of the connected and/or autonomous vehicle.

GuardKnox sees cybersecurity as the foundational layer for added levels of connectivity and personalization in connected and autonomous vehicles: enabling not only increased revenue streams per initial vehicle sale but also the end-user customization of the vehicle necessary to meet changing individual needs in a cost-effective manner.

The External-Local SNO™ Controller is completely autonomous, has high-performance data processing capabilities, does not require external connectivity, constant communication, cloud connectivity, or any on-going updates. The GuardKnox SNO™ eliminates the need for human intervention in the security mitigation process, and can defend against any kind of known or unknown cyber-attacks.

## EXTERNAL-LOCAL SNO™ CONTROLLER SPECIFICATIONS

| Component | Description |
|---|---|
| Processor | ARMv7 Cortex-M4 32-bit microcontroller |
| Memory (RAM) | Typically up to 256 KB |
| Storage (Flash) | Typically up to 1MB |
| Ports | Up to 1 x CAN 2.0B (up to 1 Mbps)<br>Up to 1 x CAN-FD (up to 8 Mbps)<br>Up to 1 x Ethernet 100 Mbps or Gigabit Ethernet<br>Up to 1 x LIN interface |
| CAN 2.0B (up to 1 Mbps) | Typically up to two interfaces per module |
| CAN-FD (up to 8 Mbps) | |
| Ethernet 100Mbps | |
| Other capabilities | LIN |
| Secure Boot | Encrypted and signed image |
| Data-at-Rest Encryption | AES128, AES256 |
| Symmetric encryption support | AES128, AES256 |
| Asymmetric encryption | RSA (up to 4096bit key size), ECC (up to 256bit) |
| Cryptographic signature | HMAC |
| Cryptographic Hash | SHA1, SHA2, SHA256 |
| Support for encrypted communication over TLS, SSL, DTLS | Yes |
| Ability to provide a complete hardware and software design | Yes |