FLEET-LEVEL TRUCKING PROTECTION

CYBERSECURTIY SOLUTIONS FOR THE **TRUCKING INDUSTRY** SEAMLESSLY INTERGRATED DURING PRODUCTION OR **RETROFITTED** IN THE **AFTERMARKET** AS A SIMPLE PLUG IN

TRUCK PROTECTION IN THE FACE OF VEHICLE HACKING

Todays trucks are heavily connected vehicles through multiple networks and automotive computers. Connectivity is changing trucking operations as every connected technology adds new cybersecurity vulnerabilities. As the industry matures towards higher levels of autonomy and levels of connectivity, the exposure is exponential. Cybersecurity needs to be viewed as a necessity rather than a luxury.

Cybersecurity should not be viewed as a 'patch in' product but rather as a holistic and determinsitic built from the ground up solution.

Robust and deterministic cybersecurity must be employed for cyber health with a defense-in-depth approach. Furthermore, the trucking industry is a pivotal player in the world economy, oftentimes carrying valuable cargo that may have far reaching negative consequences, should loss or theft of cargo occur.

CYBERSECURITY OF TRUCKS AND TRUCKING FLEETS

As trucking OEMs integrate their trucks with electronics and wireless connections, vulnerability points for hackers to exploit increase exponentially. Cybersecurity should be treated as an extension of safety in order to maintain the control and integrity of the vehicle.

Trucks and trucking OEMs are often members of traditional fleets, generating a plethora of operational data, indicative of vehicle behavior, maintenance, functionality, health and more. Advanced fleet management relies on the constant flow of accurate data directly from the vehicles to the fleet manager's data center. Successful vehicle hacking attacks could result in:

- **Costly ransomware injections**
- **Loss of command and control communication**
- **Extensive cost from loss of cargo or income**
- **Interruption in incoming data from or to vehicles**
- **Interruption in business operations and damage to brand indentity**
- **Inability to access location data and services**
- **Infiltration and exfiltration of data**
- **Inability to send over-the-air (OTA) updates**

www.guardknox.com | info@guardknox.com | 2 Hahazon St. PO Box 320, Ramla, Israel 7210202

FLEET-LEVEL TRUCKING PROTECTION

UNDERSTANDING THE NEEDS OF THE TRUCKING INDUSTRY

Trucking telematics are considered one of the biggest growth industries, expected to grow over 25% in usage within an over $42 billion industry. Telematics and fleet management solutions enable commercial trucking OEM's and large fleets to monitor, filter, and better understand usage.

Commercial trucking OEM's and large fleets can be particularly vulnerable against ransomware or malware attacks. Attacks can easily be embedded in a seemingly innocent vehicle software update file and transferred to the truck or fleet, unknowingly by its owner. It is essential that any improper command to an ECU is stopped, reported and locked down in real-time.

LOCAL SECURE NETWORK ORCHESTRATOR (SNO™)

GuardKnox's unique value proposition brings solutions to the trucking 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 trucking 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.

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 ECU:** Create the secure in-vehicle environment to ensure no vulnerability is exploited or used as a stepping stone to take control of any truck in the fleet – protecting 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