AFTERMARKET EXECUTIVE SUMMARY

CYBERSECURTIY SOLUTIONS THAT ENABLE **AFTERMARKET VENDORS** TO IMPLEMENT STATE OF THE ART **CYBERSECURITY** PROTECTION TO THEIR VEHICLES AS THE FOUNDATION FOR ADDED **SERVICES**

THE MODERN CONNECTED CAR IN THE AFTERMARKET

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

As vehicles drive toward autonomy, they multiply in complexity, becoming far more connected. Today's car is a highly sophisticated local area network on wheels that controls numerous complex systems via hundreds of micro-processors, up to 150 ECUs, and numerous sensors, interconnected by a high-speed, high-availability internal communications network. Connected vehicles transmit more than 25 gigabytes of data per hour, the equivalent of a dozen HD movies.

Just as cybersecurity is one of the biggest threats in our online lives, it is absolutely essential that we take the automotive cybersecurity issues seriously as well.

DATA MONETIZATION FOR CUSTOMIZATION AND PERSONALIZATION

The automotive **aftermarket** industry is in the midst of a paradigm shift. Drivers, and their needs, are now the focal point rather than the vehicle itself. In order to facilitate such a transition, it is imperative to not only take cybersecurity as an extension of safety, but also as an enabler to create **added value** through:

- Vehicle personalization and customization
- Revenue generation from new market streams
- Cost reductions and security and safety enhancements.

The monetization of this data is reported to add up to **$450-$750 billion** in additional revenue by 2030, it is imperative to formulate new business models built on technological innovation and advanced capabilities to monetize car-generated data into valuable products and services, all whilst maintaining the highest level of security and safety.

GUARDKNOX'S METHODOLOGY, WHICH PRIORITIZES AND PROTECTS **SAFETY-CRITICAL SYSTEMS**, HAS BEEN PROVEN IN THE ISRAELI AIR FORCE AND **ADAPTED** AND **OPTIMIZED** FOR THE MODERN **AFTERMARKET INDUSTRY**

AFTERMARKET EXECUTIVE SUMMARY

FIGHTERJET LEVEL PROTECTION WITH AN AUTOMOTIVE PRICE TAG

The GuardKnox team brings over two decades of experience creating and implementing innovative, military-grade, hardware cybersecurity solutions. The GuardKnox technology is based on the patented **Communication Lockdown™ Methodology,** which is successfully deployed in Israel's F-35I and F-16I fighter jets, as well as the Iron Dome and the Arrow III missile defense systems. We have adapted this same approach to security and safety for the automotive industry.

Computer industry solutions such as Intrusion Detection/Intrusion Prevention Systems (IDS/IPS) and/or firewalls may seem to be the obvious choice to protect computers-on-wheels, but they are oftentime ill-equipped to meet the cybersecurity needs of the automotive industry.

The holistic approach facilitates 99.9999% reliability and **zero** false positives. There is absolutely no room for error or false positives, for example, malfunctioning of breaks when

GUARDKNOS'S UNIQUE **VALUE PROPOSITION** BRINGS SOLUTIONS TO THE INDUSTRY THAT PARSE ALL IN-VEHICLE COMMUNICATIONS AND DROPS ANY IMPROPER MESSAGES IN REALTIME. OUR PLATFORM PROVIDES A **SECURE END POINT** FOR DATA HOSTING, PROCESSING AND STORING

EXTERNAL SECURE NETWORK ORCHESTRATOR (SNO™)

The Secure Network Orchestrator (SNO™) is a comprehensive product that provides protection and security as the foundational layer for additional levels of connectivity.

The External SNO™ locks down and secures any single ECU with external connectivity. Ideal for telematics, infotainments, on-board diagnostics, fleet management and more, it is seamlessly integrated during production or retrofitted as a simple plug-in to the OBD port.

Important vehicle metrics and relevant predictive maintenance data can be sent back to manufacturer's operational data centers in order to facilitate customer relationships and offer value-added services based on driver behavior and preferences.

USE CASES

RKE & Secure Key Storage: Enable your dealership to be completely secure and go "keys free" with no more downtime

Inventory Management: Understand necessary predictive maintenance, location, and other critical details to maximize your fleet performance

Reporting & Retention: Under fleet analytics and other vehicle based information - report securely to SOC