GUARDKNOX

HOW AUTO INSURERS CAN PROTECT THEMSELVES FROM THE BILLION-DOLLAR CYBERCRIME INDUSTRY

ENABLES DATA ANALYTICS & MONETIZATION ACROSS THE INSURANCE ECOSYSTEM

HIGHLIGHTS

□ Ransomware is expected to cost $250 billion USD by 2031 globally.

□ Connected fleets and high-end vehicles are “computers on wheels” that can serve as attractive targets for ransomware and cyberattacks that result in vehicle theft, data theft and even endanger the lives of vehicle occupants

□ GuardKnox and its partners mitigate the exposure of insurance companies with an end-to-end automotive cybersecurity solution

□ Automotive cybersecurity can also enable new revenue streams via ransomware insurance policies, discounted premiums from telematics driving data and other services

THE CHALLENGE

Defining the threats and prioritizing protection must be done from the outset, before destructive consequences ensue. Furthermore, stringent protection is imperative to ensure that no single vulnerability in a vehicle is exploited and used as a stepping stone to take control over an entire fleet.

Ransomware is a rapidly-growing "industry", generating $250 billion by 2031 from US businesses. Since cleanup costs and lost revenues can be up to 100-200 times greater than the ransom itself, it's no surprise that 45% of ransomware victims and/or their insurance companies pay the ransom. The May 2019 ransomware attack on the City of Baltimore, Maryland is a case in point. At the behest of the FBI, the city did not pay the 13 Bitcoin ransom (about $100,000) but non-payment cost the city nearly $18 million in clean-up costs and lost revenues.

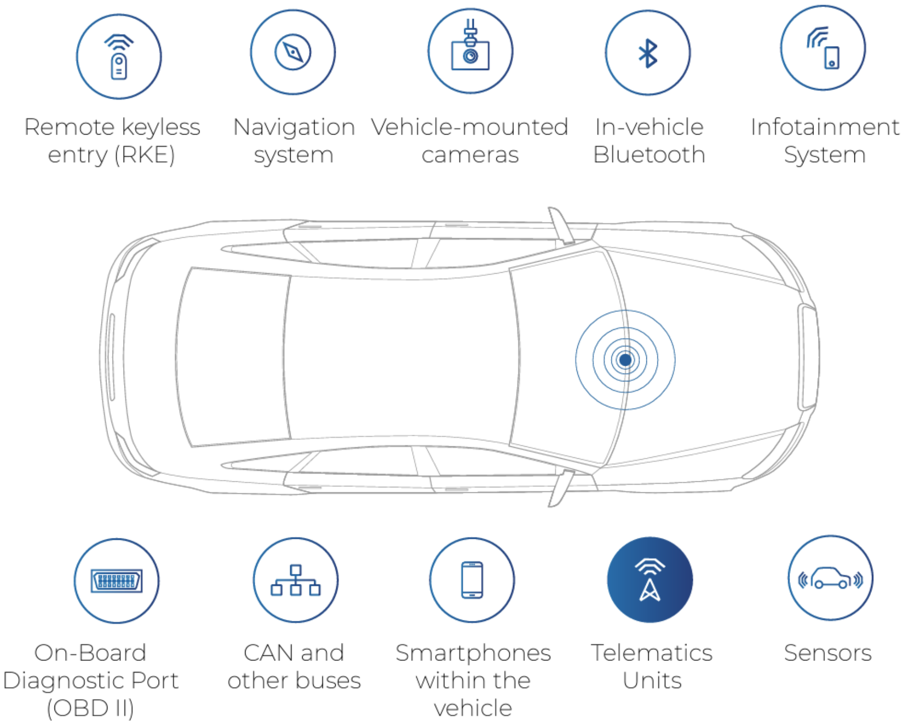
On the other hand, the town of Lake City, Florida, fell victim to ransomware in June 2019 and paid a ransom of 42 Bitcoin (about $490,000). The city paid $10,000 while their insurance company paid the remainder. About two weeks later, another small Florida town paid a $600,000 ransom in Bitcoin.

While computer networks of businesses and governmental organizations of all types continue to fall prey to ransomware and other cyberattacks, connected fleets and high-end vehicles are "computers-on-wheels" that comprise a potentially highly profitable new market for a variety of cyberthieves.

The potential for cyberhijacking of vehicles was already proven in 2015 when a Jeep Cherokee, was driven off a highway by white-hat hackers Charlie Miller and Chris Valasek. To date, the biggest challenges for vehicle hackers have been monetization and scale, but fleet owners, wealthy individuals and their insurance companies cannot wait until ransomware attacks on vehicles become as commonplace as ransomware attacks on municipal and corporate networks.

LOCATING THE PRIMARY ATTACK SERVICE

While a connected vehicle has nearly 150 computers or “ECUs” only about 10 ECUs are considered high-risk due to their connectivity to external networks via the Internet. Until now, vehicle hacking has required a significant investment of time, expertise, and money—and targeting specific vehicles is no easy task.



But vehicle fleets or high-end connected vehicles could offer the high ROI that will incentivize hackers to invest the time to overcome the remaining obstacles.

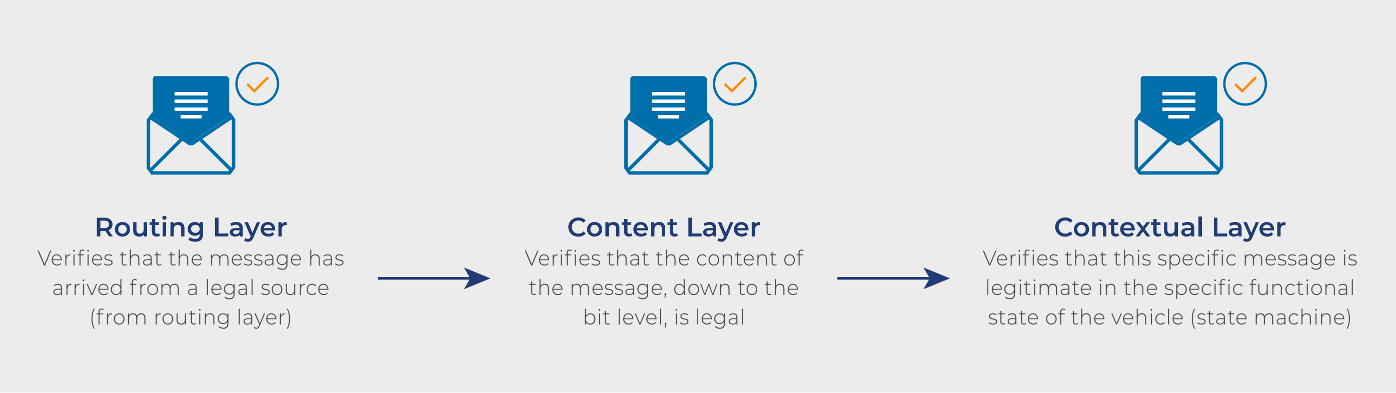
[Fleet Management Systems (FMS)] offer a much larger, more vulnerable attack surface than a single fast-moving Jeep on the highway. Used by carmakers /OEMs, fleet owners and insurance companies, Fleet Management Systems provide real-time information on vehicle usage and performance.

Fleet Management Systems (FMS) offer a much larger, more vulnerable attack surface than a single fast-moving Jeep on the highway. Used by carmakers /OEMs, fleet owners and insurance companies, Fleet Management Systems provide real-time information on vehicle usage and performance. With access to the Telematics ECU inside the vehicle, a successful hack of the remote Fleet Management System could provide direct access to the Telematics ECU inside whole fleets of commercial vehicles or high-end vehicles that could result in:

- Costly ransomware injections
- Loss of command and control communication with vehicles
- Extensive cost and adverse effects of loss of cargo / income
- Infiltration and exfiltration of personal and financial data
- Regulatory investigation expenses and/or fines
- Damage to the brand or reputation of the business
- Cost of reporting the problem or data breach to customers
- Network clean-up and much, much more.

THE GUARDKNOX SOLUTION:
FIGHTER JET CYBERSECURITY FOR THE CONNECTED VEHICLE

The GuardKnox Product Line is a family of secured solutions that protect against any type of known and unknown cyberattack. Requiring neither external connectivity nor on-going updates, the GuardKnox solution is completely autonomous and uses a patented Communication Lockdown™ Methodology to inspect and verify all vehicle network traffic on three levels:



Routing Layer
Verifies that the message has arrived from a legal source (from routing layer)

Content Layer
Verifies that the content of the message, down to the bit level, is legal

Contextual Layer
Verifies that this specific message is legitimate in the specific functional state of the vehicle (state machine)

Adhering to the most stringent security and safety standards, including ISO 26262 and ISO 15118, the GuardKnox product line comprises the:

- GuardKnox CommEngine is a single-chip solution with a safe and secure design that performs routing actions using hardware to allow for ultra-low latency and multi-gigabit bandwidth, addressing current automotive needs in connectivity and scalability.
- GuardKnox SOA Framework provides OEMs, Tier 1 Suppliers and aftermarket vendors a secure in-vehicle landing point to download and host services and applications with secure separation and full access control.
- GuardKnox Aftermarket Add-On serves as a connectivity Domain Controller gateway to external communication by wireless and wired interfaces.

EASY INSTALLATION IN THE AFTERMARKET

The easy installation of GuardKnox cybersecurity solutions behind the OBD port, reduces the risk of ransomware infection of fleet vehicles or vehicle hijacking that can result in cargo loss, costly downtime, or even loss of life. Securing the telematics and fleet management system can mitigate risk and reduce payouts by insurance companies.

GuardKnox not only provides stringent cyber protection, but also secures brand reputation and accurate business processes that can be derailed from costly cyberthreats.

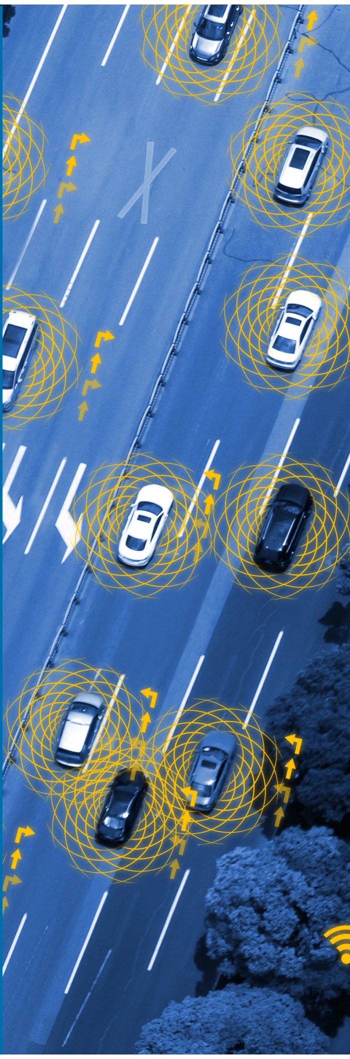
The External SNO™ is an especially attractive solution for meeting the needs of the insurance industry. Like alarms and immobilizers, it can be retrofitted to the vehicle as a simple plug-in aftermarket solution, fitting seamlessly into the automotive value chain without third-party integration.

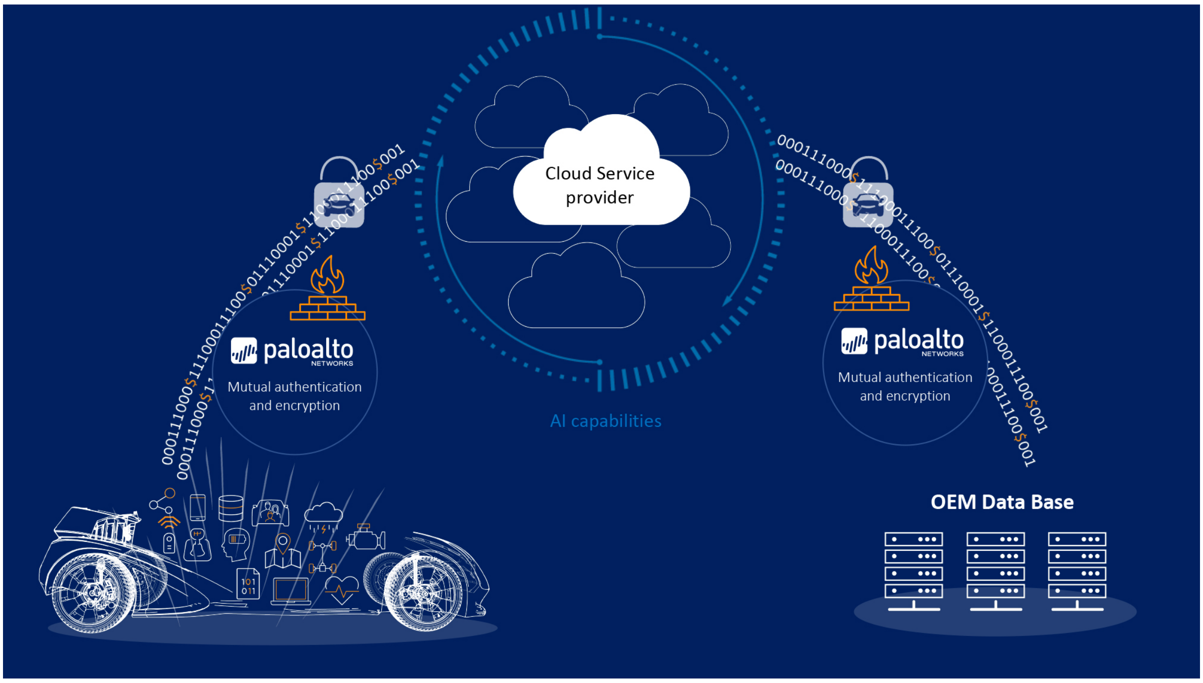
GUARDKNOX AND LEADING INDUSTRY PARTNERS PROVIDE END-TO-END CYBERSECURITY

paloalto NETWORKS

GuardKnox and Palo Alto Networks® provide a joint end-to-end cybersecurity solution for the automotive and insurance industries that combines GuardKnox's Communication Lockdown protection with the Palo Alto Networks® GlobalProtect™ secure communication channel.

Palo Alto Networks® provides the encrypted communication channel for telematics and other data that is shared between the vehicle and remote databases at OEMs, fleet management companies, and insurance companies while GuardKnox protects the internal vehicle systems from hackers and ransomware.





DXC TECHNOLOGY

DXC TECHNOLOGY

GuardKnox and DXC Technology, a world leading IT services company, have demonstrated real-time monitoring of fleets and fleet cyberhealth. The two companies are collaborating to secure and monitor the data traffic between the car and the operational back end, or security operations center (SOC). The GuardKnox SNOTM transmits relevant data and enables real-time monitoring and in-depth analysis of security-related events. SOC analysts are presented with well defined, targeted and actionable intelligence which enables UBI models, optimized fleet maintenance forecast, etc.

USE CASE #1

PROTECTING VEHICLE FLEETS AGAINST RANSOMWARE

Challenge

Fleet Management Systems offer large attack surfaces with access to numerous vehicles that offer sizeable ROI for cyberthieves and hackers of the fast-growing $8 billion ransomware industry. Successful attacks can result in fleet level loss of command and control, loss of vehicle operation and cargo, data theft, damage to brand, network clean-up costs and much, much more.

Solution

Installing the GuardKnox solution in the aftermarket protects in-vehicle networks from ransomware and other cyberattacks. In addition, it can be used for on-board data processing and storage to support added services such as telematics for predictive maintenance programs and data analytics. For end-to-end coverage, insurance companies and fleet owners can secure all communications between the central Fleet Management Systems and the in-vehicle Telematics ECU protected by GuardKnox solutions.

Benefits

GuardKnox-hosted telematics can potentially provide highly relevant data for identifying dangerous or safe drivers and help insurance providers adjust their insurance rates accordingly. Furthermore, the GuardKnox platform has the functionality to not only host data, but also retrieve, process and transmit relevant data, saving time and extensively reducing costs.

Insurance providers can offer incentivized policies under the condition of installation of the GuardKnox solution, not only prohibiting access to the entire fleet, but provide data that helps assess personal or regional risks by identifying locations and times-of-day that are high-risk for accidents and lets insurers adjust policy prices—and discounts—accordingly.

USE CASE #2

SECURING HIGH-END CONNECTED VEHICLES

Challenge

High-end connected vehicles like the Mercedes Benz SLS Electric Gullwing E-Cell or the Rolls Royce Phantom 102EX Electric Car have price tags of $ 1 million or more. As highly exclusive electric vehicles that are not easily replaced, their owners will be very likely to pay a ransom.

Solution

Installing the GuardKnox solution in the aftermarket will protect the vehicle from the injection of ransomware and outright theft via hacking from the cellular Internet used by telematics and other connected vehicle ECUs.

Benefits

The GuardKnox solution is easily installed by the aftermarket, whether at car dealerships or general aftermarket installers. In addition to its ability to autonomously prevent ransomware attacks, the GuardKnox solution can prevent vehicle theft from hacking the immobilizer and assist in recovering stolen vehicles by enabling the GPS to operate after the theft of the vehicle.

For more information on how GuardKnox enables protection and new revenue-generating channels for insurance providers, click here.

About GuardKnox

GuardKnox is a leading automotive technology company ushering in the smartphonization of the next generation of vehicles by building high-performance, service-oriented, customizable, and secure-by-design products for the next generation of driver-centric mobility. GuardKnox enables the software-defined vehicle with scalable and flexible technologies necessary for full-connectivity and empowers consumers with the ability to customize their vehicle's performance, as well as their in-vehicle experience. Founded in 2016, GuardKnox is based in Israel, with subsidiary locations in Munich, Germany, and Detroit, Michigan.