Automotive Cybersecurity Solution by
PALO ALTO NETWORKS© & GUARDKNOX

Highlights

- Palo Alto Networks© and GuardKnox have teamed up to provide an end-to-end cybersecurity solution for the modern connected vehicle.
- By using Palo Alto Networks'© expertise in network and cloud security and worldwide infrastructure with GuardKnox's expertise in automotive security and innovative technology, OEM vendors can secure the over-the-air (OTA) communication between the vehicle, the cloud, and their operational centers.
- The joint solution is an enabler for a variety of new services that depend on secured transmission of information between service providers or operational centers and the vehicles.
- The GuardKnox and Palo Alto Networks© joint solution provides the end-to-end cybersecurity solution that is critical for the continued growth of the connected/ autonomous vehicle industry.

The Challenge

The modern vehicle features 100-150 computers called “ECUs” that communicate with one another via numerous protocols and networks. When a vehicle is hacked, it can jeopardize the safety of passengers. Vehicle hacking can lead to very expensive recalls as well as product liability claims or even class action suits. In addition to the in-vehicle threat, hackers can potentially gain access to the channel between the ECU and the cloud that is the basis for the communication between the OEM and the updating vehicle functionality. This channel is also a potential security gap through which hackers could gain control on the vehicle.

A vehicle over-the-air (OTA) software update brings another attack surface when there is direct external communication directly with a variety of ECUs. Robust, end-to-end security for external communications is absolutely imperative for protecting against OTA hacking as well as against regular on-going communication over the Internet that can endanger both the security of the vehicle and the physical safety of passengers. As such, OEM manufacturers and fleet owners must be able to detect and stop these vehicular cyber-threats in real time while retaining the ability to continuously and securely communicate with the vehicle.

Cybersecurity threats to vehicles are increasing as cars become more connected.

GuardKnox Automotive Cybersecurity

The GuardKnox solution, prevents cyber-attacks in real time eliminating false positives.

Seamlessly incorporated during vehicle production or during aftermarket, the GuardKnox platform parses all messages in the vehicle and those entering the vehicle's network. GuardKnox's Communication Lockdown™ methodology provides the highest level of vehicle security by permitting only authorized communication, examining their routing, content, and contextual layers and locking every bit in every field in every message within the vehicle to prevent unauthorized manipulation. By utilizing these strict rule sets and state machine, the architecture is designed to transmit only the vetted communication with the highest degree of security and fidelity, making the system formally verifiable, efficient, and highly resistant to attack.

The solution also includes a reporting mechanism that provides centralized fleet security. As a complete solution, the GuardKnox platform seamlessly integrates into the vehicle, the value chain, and the entire vehicle production process i.e. software and hardware.

Another innovative patented technology of GuardKnox is Service Oriented Architecture (SOA) in vehicle computers. This architecture brings the ability to securely run different applications that use different operating systems in parallel in real time and still be secured by GuardKnox security core and architecture. All GuardKnox product lines provide in vehicle security, enabling secured storage and secure processing, complying with GDPR and by that also securing Over The Air (OTA) updates.

The GuardKnox product family is comprised of:

- High-Performance Communication Engine in hardware
- Secure Service-Oriented Architecture Framework (SOA)
- Aftermarket Add-On Tailored Solution
- Cybersecurity Solutions

Palo Alto Networks©

The Palo Alto Networks© Security Operating Platform prevents successful cyber-attacks through intelligent automation.

The platform combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection and prevent cyber breaches from the cloud to the vehicle.

GlobalProtect™ Cloud Service for the connected vehicle extends Palo Alto Networks'© Security Operating Platform to the connected vehicle by leveraging a cloud-based security infrastructure managed by Palo Alto Networks©. Using Panorama™ network security management, you can create and deploy consistent security policies across your entire fleet of vehicles without the challenges of sizing firewalls, computing resource allocations or minimizing coverage gaps. GlobalProtect™ Cloud Service for the connected vehicle scales as demand shifts and traffic patterns change.

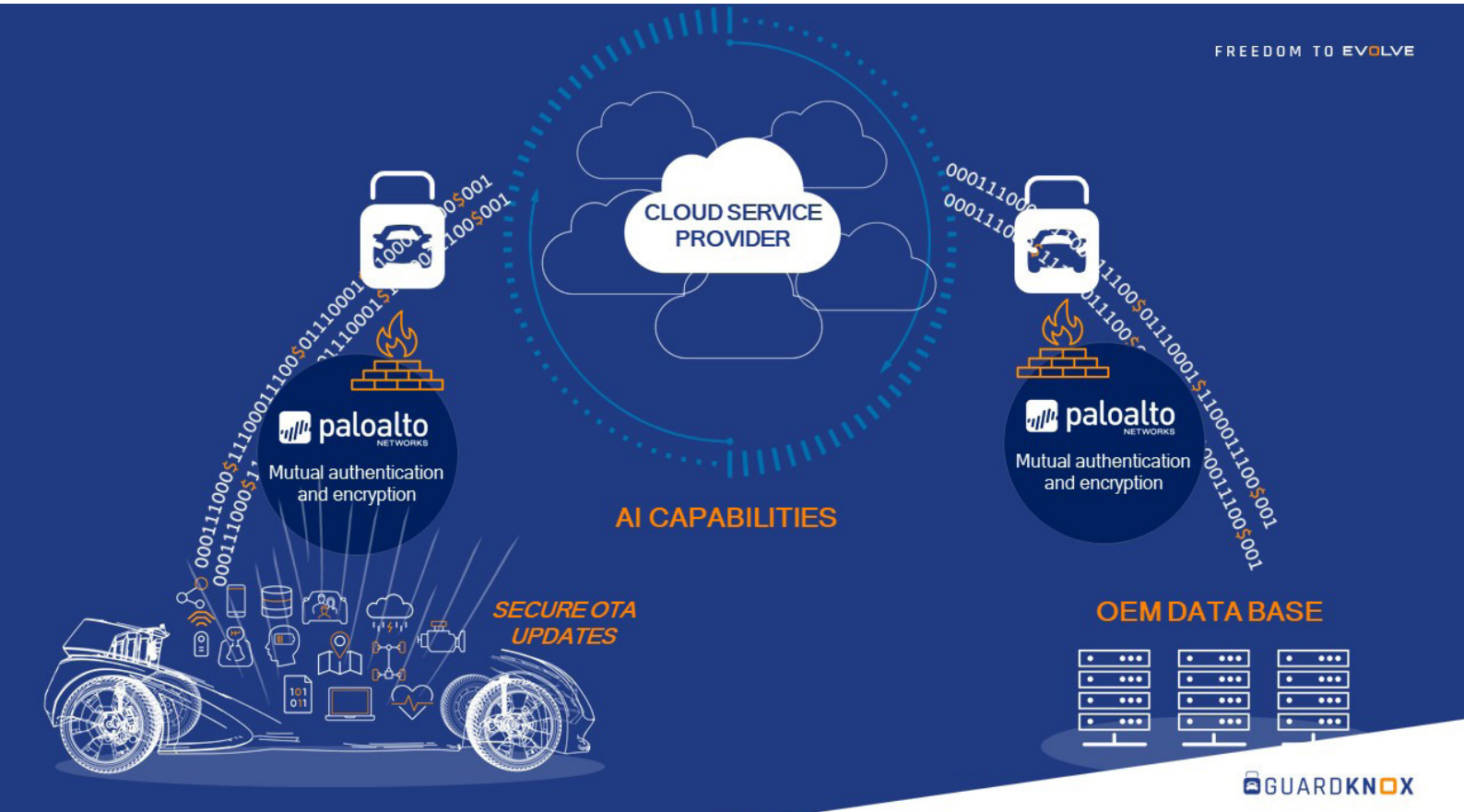
All GlobalProtect™ Cloud Service cloud service locations are connected through a full mesh VPN without the complexity of configuration, since an SSL VPN connection is required from the connected vehicle to the cloud or form the cloud to the connected vehicle.

A shared network ownership model reduces the operational burden of deploying GlobalProtect ™ Cloud Service security to connected vehicles. Palo Alto Networks© manages the cloud network infrastructure, ensuring reliability, scalability and availability while the OEM, fleet management company or dealership focuses their efforts on deployment.

Palo Alto Networks© & GuardKnox's Communication Lockdown™ Automotive Security

The Palo Alto Networks© and GuardKnox partnership and joint solution creates an End-to-End cybersecurity solution combining secure in-vehicle communication lockdown with secure communication between the vehicle and remote databases at OEMs, fleet management companies, car dealerships and more e.g. connecting to the OEM app store.

Smart vehicles are connected to the Internet for a variety of applications including navigation, infotainment, over-the-air (OTA) vehicle software updates and more. Unsecured connections could enable hackers to manipulate the data during transfer in order to steal personal information, overcome a vehicle's security mechanisms or even take control of the car. As such it is imperative to have an end-to-end cybersecurity system that can ensure the integrity and security of both the internal and external vehicle networks.



Palo Alto Networks© GlobalProtect™ Cloud Service secures the external network between the vehicle and the OEM cloud through the use of their secured communication channel while GuardKnox provides a holistic lockdown approach to the vehicle's internal network by enforcing strict set of rules on all incoming and outgoing communication in real time.

The collaborative solution uses NSA Suite B Cryptography in order to deliver the highest level of end-to-end security while still enabling the GlobalProtect™ Cloud Service firewall to effectively filter and monitor the traffic. Privacy and confidentiality are maintained by using Advanced Encryption Standard (AES) encryption and the exchange of encryption keys uses the state-of-the-art Elliptic Curve Diffie–Hellman (ECDH) protocol and is authenticated using Elliptic Curve Digital Signature Algorithm (ECDSA) or the well-established RSA public key infrastructure.

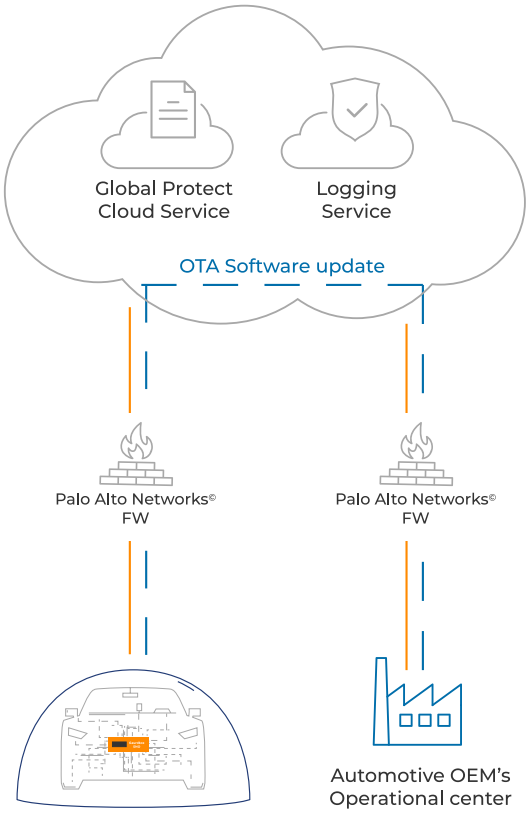
The joint solution between Palo Alto Networks© and GuardKnox ensures the highest caliber of security across the entire spectrum of communication from within the vehicle all the way to the cloud of the OEM, fleet management company, telematics provider, insurance provider, emergency service, and more. This ensures that the connected car can leverage the efficiencies and conveniences offered by the Internet, including but not limited to secure OTA for vehicle features or value added services, command and control engine tuning, and secure real-time fleet analytics.

Use Case # 1

Securing On-Going Communications Between OEMs and Vehicles

The Challenge:

OEMs are seeking an end-to-end solution to securely and safely communicate with their vehicles to make software changes and OTA updates in real time. Without mutual authentication and encryption over a secure channel and without a secure destination within the vehicle, this process is a proven target for cyberattacks.



Solution:

The fully integrated Palo Alto Networks© and GuardKnox solution offers end-to-end cybersecurity, combining external communication with secure in-vehicle communication lockdown. The Palo Alto Networks© next-generation firewall supports both mutual authentication and the highest levels of encryption from the OEM's cloud to the vehicle. GuardKnox's patented hardware and software solution locks down all internal network communication, ensuring the complete security of the vehicle. In addition, GuardKnox serves as a platform within the vehicle for secure on-board data storage and processing, as well as secure application hosting through its Services Oriented Architecture (SOA).

Benefits:

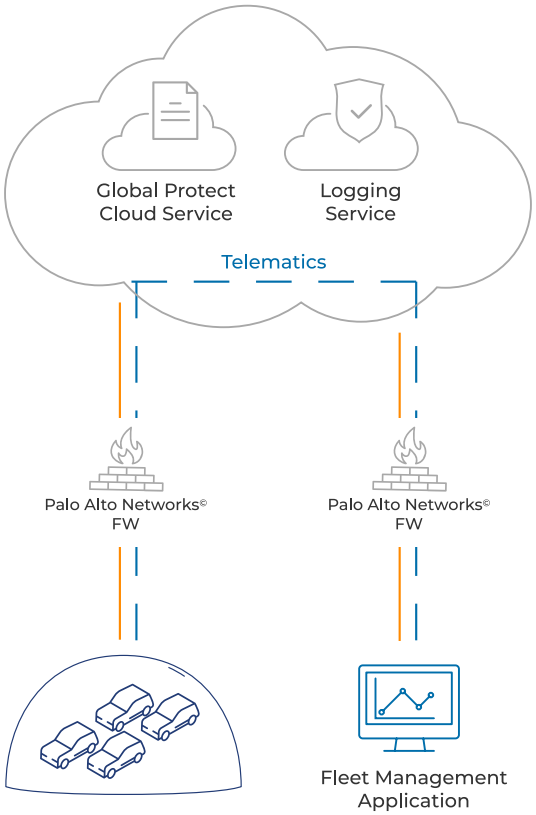
The fully integrated and mutually authenticated Palo Alto Networks© and GuardKnox solution enables OEMs to save time and money by integrating a single end-to-end solution for securing periodic OTA maintenance and new feature updates as well as ongoing, real-time communication. The solution also facilitates an entirely new set of advanced functions for manufacturers to receive data regarding the driving habits and preferences of multiple drivers of the same vehicle and remotely configure and personalize functionality such as engine tuning, gear shifting, suspension performance etc. The joint solution prevents threats to the car and enables control of bidirectional traffic. OEM manufacturers now have a way to prevent threats from: attacking a car, hacking the car, attacking the DB or back end systems. With the joint solution sensitive data can be kept secure.

Use Case # 2

Securing Communications Between Vehicles and Database Applications

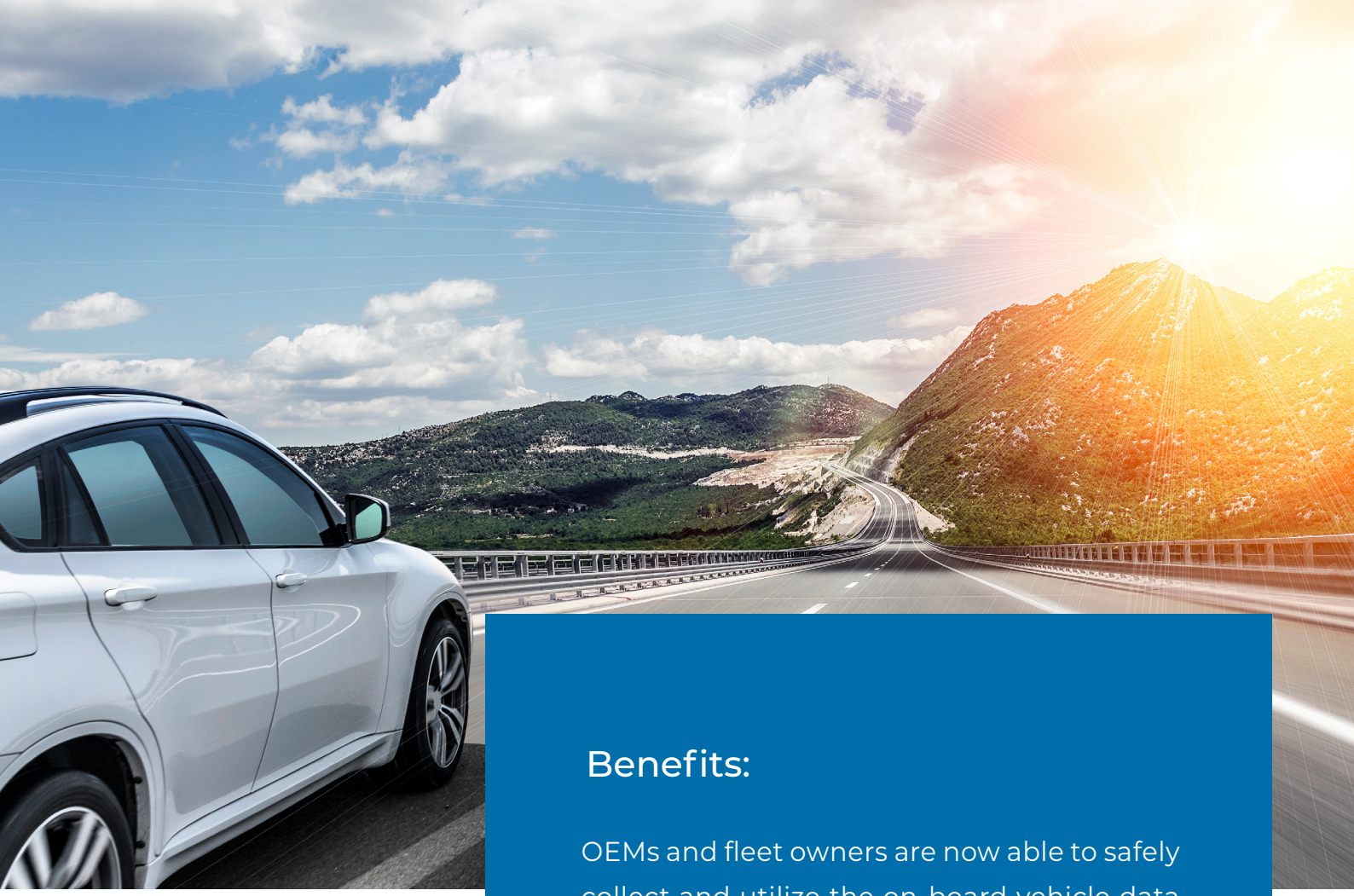
The Challenge:

Cars generate more useful data today than ever before. The data may relate to vehicle usage, vehicle maintenance, driver behavior, vehicle location, etc. This information is invaluable for fleet owners and car manufacturers who can use such data to provide services such as fleet management, vehicle maintenance and inventory management. Unfortunately, today only a fraction of the data is used in real-time, due to the complexity of implementing and securing the communication channel between the vehicles on the road and the OEM's backend systems or fleet operations centers.



Solution:

GuardKnox and Palo Alto Networks' end-to-end solution allows for data to be securely transmitted between a vehicle and a central database, whether owned by an OEM, fleet managing company, or a service provider such as a ride-sharing company. Palo Alto Networks secures the external communications channel by which the data is transmitted, while GuardKnox secures the in-vehicle communications, locking down all internal communication in the vehicle and securing any external communication that comes into the vehicle. The GuardKnox device also serves as an on-board secure data storage and processing system.



Benefits:

OEMs and fleet owners are now able to safely collect and utilize the on-board vehicle data to enable real-time, fleet-level analytics. Preventing cyberattacks with the integrated GuardKnox and Palo Alto Networks© solution ensures the safe growth of the telematics and fleet management systems industry and allows OEMs, fleet owners and other service providers to reduce their business costs while improving their customer service.

About GuardKnox

GuardKnox is a technology and engineering company specializing in E/E products and solutions for the automotive market.

GuardKnox is the automotive industry's first Cybertech Tier Supplier empowering OEMs, Tier 1 suppliers, and the aftermarket to deliver the next generation of software-defined and service-oriented vehicles. GuardKnox's flexible and scalable solutions enable added connectivity, Zonal E/E Architecture, hosted applications, high-speed routing (including network recovery and service discovery functionalities), vehicle personalization, and security.

The company's pioneering approach to automotive innovation is inspired by technology from the aviation industry, providing GuardKnox with the experience needed to develop secure, high-performance computing solutions using a patented Service-Oriented Architecture (SOA).

Founded in 2016, GuardKnox is based in Israel, with subsidiary locations in Stuttgart, Germany, and Detroit, Michigan.

Find out more at https://www.guardknox.com

About Palo Alto Networks©

Palo Alto is the global cybersecurity leader known for always challenging the security status quo. Its mission is to protect our way of life in the digital age by successfully preventing cyberattacks. This has given it the privilege of safely enabling tens of thousands of organizations and their customers. The company's pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers, Palo Alto provides highly effective and innovative cybersecurity across clouds, networks, mobile devices and connected vehicles.

Find out more at www.paloaltonetworks.com.