FROST & SULLIVAN

GuardKNOX Cyber Technologies

2018 European Vehicle Cybersecurity for Automotive Technology Innovation Award

2018
BEST PRACTICES
AWARDS

Contents

Background and Company Performance

Industry Challenges

The growth of connected vehicles across the globe is exponentially increasing the risk for potential cyber-attacks in the industry. Since these connected cars generate large amounts of vehicle and customer data every day, an intruder gaining access to a vehicle's computers - Electronic Control Unit (ECUs) will both risk the safety of the passengers and tarnish the brand reputation of original equipment manufacturers (OEMs). As a result, OEMs are beginning to look for ways to address the prevailing challenges of the automotive cybersecurity market.

Because the automotive supply chain is extremely fragmented, coordinating a common cybersecurity strategy throughout the value chain will be complex and challenging. Increasing vehicle connectivity poses the biggest cybersecurity challenge in the industry. In-vehicle communication extends from infotainment to mobile-based communication (leveraging 4G and 5G), voice recognition, navigation, and communication with other vehicles and infrastructure. Connectivity with external devices multiplies threat vectors and increases product vulnerability, which in turn exposes vehicles and sensitive data to hackers. Cybersecurity solutions should be designed in a way that keeps all of the possible attack surfaces in mind.

The evolving threat landscape possesses significant challenges for OEMs to secure connected vehicles from both current and future potential attacks. OEMs are implementing Over-The-Air (OTA) updates to send security patches in case of future vulnerabilities. It is important to establish a secure communication protocol for distributing OTA updates, otherwise, it could open up additional attack surfaces for hackers.

The automotive industry must impose strict guidelines, establish tough safety standards, and take cybersecurity cues from both specialist security companies and cross industry experts to implement the highest level of security in vehicles. It is important for OEMs to identify the customer's pain points and collaborate with specialist companies in order to build secure autonomous vehicles.

GuardKnox is uniquely positioned to address the majority of challenges prevailing in the automotive cybersecurity market. Because GuardKnox's patented cybersecurity solution, a Secure Network Orchestrator (SNO), is offered as a plug-in hardware and software component, it can be seamlessly integrated during vehicle production. This solution works using a Communication Lockdown™ Methodology which requires all the messages entering into the vehicle's network to pass through routing, content, and contextual layers. These layers work to proactively stop vulnerable messages before they are sent to ECUs, thereby offering resiliency to harmful cyber-attacks. The Central SNO solution offered by GuardKnox provides another layer of in-vehicle communication cyber security therefore bringing a security in-depth approach to the automotive industry.

Technology Attributes and Future Business Value

GuardKnox Cyber Technologies is based out of Israel and is a cybersecurity solutions provider for connected and autonomous vehicles that was founded by Moshe Shlisel (CEO), Dionis Teshler (CTO), and Idan Nadav (Chief Engineer) in 2015. Following decades in the Israeli Air Force, the team wanted to develop a cybersecurity solution for the automotive industry that was similar to those used in fighter jets. GuardKnox's patented Communication Lockdown™ Methodology was inspired by the GuardKnox team's success in Israel's F-35I and F-16I fighter jets, as well as the Iron Dome and the Arrow III missile defense systems. GuardKnox solutions are developed according to the most stringent cyber security standard - Common Criteria (ISO 15408) which was developed by the NSA.

Criteria 1: Product Impact & Industry Impact

GuardKnox Patented Communication Lockdown™ Methodology (US Patent 9,899,563B2) follows a centralized approach that locks down all of a vehicle's internal network communications. The messages entering into the vehicle's network will pass through real-time pre-defined set of rules and standards for authorization. If the requirements are not met, the message is classified as invalid and will not be permitted into the network. Lockdown methodology provides the highest level of vehicle security by permitting only authorized communication, locking every bit in every field in every message within the vehicle, discarding any type of inappropriate transmission. Finally, the GuardKnox SNO provides a contextual based security which enforces the pre-defined state machine rule-set.

GuardKnox's second patent for hardware architecture (US Patent 20,180,131,697)—Secure Network Orchestrator (SNO)—enables secure physical separation of communication networks. SNO will lock down all internal communication on a bit level and serves as a gate keeper by enforcing the layers of protection on every message either ingress or egress. GuardKnox solutions and its unique position of in-vehicle architecture provides full coverage of all communication with all ECUs. It is more applicable to the fragmented automotive supply chain because it eliminates the complexities of integrating software-only solutions into a holistic security strategy. This hardware component can be seamlessly integrated in production or aftermarket as a plug-in. SNO also enables real-time customization by providing secure hosting of additional applications and services.

GuardKnox's third patent for Service Oriented Architecture or SOA (US Patent 15,863,053) allows for a SOA to support GuardKnox's already patented Lockdown Methodology for vehicle cybersecurity. This patent 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. It also has a secure separation (both hardware and software) between all resources, application groups, and operating systems.

This patent brings GuardKnox to the heart of the paradigm shift the automotive industry is experiencing - the vehicle will become a platform for services, quite similar to smartphones.

GuardKnox's innovative Communication Lockdown™ approach and hardware architecture will provide an enhanced level of security in connected vehicles, eliminating integration overheads for OEMs, lowering complexity issues, and reducing overall cost. GuardKnox stands out in the market by offering a stand-alone gateway unit that not only secures the vehicle but also can enable real-time customization, securely host services, and have on-board secure storage and secure processing that complies to GDPR. GuardKnox's technology ultimately becomes the cyber security foundation of the vehicle.

Criteria 2: Scalability

Future cybersecurity solutions must be robust, standalone, and agnostic. GuardKnox's product is a standalone component that is scalable across different communication protocols within the vehicle network, such as Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST), and Ethernet. The GuardKnox SNO works well in any closed communication environment with finite group of messages. GuardKnox solutions are scalable throughout the life cycle of the vehicle because it has the ability to add new functionalities/applications dynamically, modify to fit the needs of the client, and adapt when OEMS change their communication networks within the vehicle.

Criteria 3: Visionary Innovation

A modern vehicle has more than 7 different networks operating with various protocols. These networks interconnect with various subsystems through a gateway ECU. The challenge is to orchestrate secure connectivity between different networks within the vehicles. Many competitors in the market are trying to provide end-to-end holistic solutions, whereas GuardKnox Communication Lockdown Methodology distinguishes itself from its competitors by protecting all messages which exist in the vehicle in real-time on a bit level - the highest resolution available. In this manner the methodology prevents any existing or future attacks. That unique approach uses a proactive approach that can be proven by an external lab that it is secured and does not require cloud connectivity. This methodology has a core finite state machine (with pre-defined rulesets) where no new state is possible and erroneous states are treated in real time to immediately reverse to a secure state and resume operations. Each ruleset defines the state of the machine and its ECUs and a list of approved messages for this specific state. Once GuardKnox, based on the OEM communication matrix (the full list of the messages in the vehicle), defines the relevant ruleset, it is automatically compiled into a state machine through an automatic dedicated ruleset generation tool developed by GuardKnox. GuardKnox maintains real-time history of previous messages to make sure the right message is sent at the right time to the right ECU with the right command. If vulnerability is detected, the message is discarded.

This methodology is completely static and different from existing learning security solutions, which change their mode of operation as they learn. Moreover, being non-deterministic cannot comply with safety and security standards because learning solutions cannot be formally verified. Communication Lockdown Methodology allows for formal verification with stringent standards of security and safety. By utilizing strict rulesets, the architecture is designed to permit only the allowed communication with very high security and fidelity. OEMs expect a reliability of 99.99999% during a vehicle operation, and this type of methodology that makes a system verifiable, efficient, and highly attack resistant meets this level of reliability.

Criteria 4: Customer Acquisition

By 2025, nearly 75% of the cars on road will be connected and will therefore be highly vulnerable. As such, OEMs demand strong security solutions that work well in almost all threat scenarios while enabling a seamless integrated system. GuardKnox's patented SNO is a standalone certified hardware and software component that can be deployed directly into vehicles, thereby eliminating complicated integration processes that are typical of current software solutions. The SNO is designed as a tamper proof black box and requires zero maintenance (except replacement if broken) and zero security updates. With changing technological innovations, the SNO can also be easily scalable for future security features. These factors are a huge competitive advantage for GuardKnox when acquiring new customers and retaining its existing customers in the industry.

GuardKnox is currently piloting its SNO with three companies—Porsche, Daimler, and DXC Technology. GuardKnox is working with Porsche to deploy SNO to protect communication channels within its vehicles from cyber-attacks. Mercedes-Benz Accessories GMBH, subsidiary of Daimler, has partnered with GuardKnox to protect its wireless communication interface and to securely connect accessories within vehicles (such as voice assistants or wireless speakers). Apart from automotive OEMs, GuardKnox also works with service companies such as DXC to offer end-to-end cybersecurity services for consumers. DXC Technology partnered with GuardKnox to secure and monitor data traffic between cars and provide real-time threat analysis. This will enable OEMs and fleet managers to monitor vehicles in real-time, detect new threat patterns, mitigate risk strategies, and alert drivers before the threats become severe. GuardKnox is also working with companies such as Liebherr, Hella, Palo Alto Networks, Bosch, DAF, Audi, and Volkswagen for vehicle cybersecurity solutions.

Criteria 5: Brand Loyalty

With digitization of vehicles, every OEM in the automotive supply chain understands that constant communication with the customer is the key to brand loyalty and increased revenues. It is important to keep the customers informed about what is happening in real time, such as vehicle tracking, theft notification, end of warranty notification, and in-vehicle maintenance reports. Currently, the biggest hurdle faced by OEMs is that they are

unable to securely provide connected services to the customer. GuardKnox's Service Oriented Architecture (SOA) provides a secure communication channel that allows OEMs to monetize, on a recurring basis, the different services a driver (customer) can use throughout the vehicle life cycle. GuardKnox recently received its third patent for SOA. Using GuardKnox's patented technology, an OEM will be able to use SOA while ensuring the highest level of protection from cyber-attacks and not jeopardizing passenger safety. This enables OEMs to stay securely connected with their customers, thereby increasing brand loyalty.

Conclusion

Connected vehicles are prone to serious cyber threats and should have the highest level of security framework within them. GuardKnox has been awarded three patents for its unique cybersecurity technology—SNO Hardware architecture, Lockdown Methodology, and SOA. GuardKnox SNO is a stand-alone hardware and software component and can be seamlessly integrated across the automotive value chain. GuardKnox's patented cybersecurity framework prevents cyber-attacks in real time with zero false positives, minimal maintenance efforts, zero connectivity requirements, and negligible performance impact, thereby increasing OEM reliability to 99.99999%. With its patented cybersecurity technologies, innovative features, and strong overall security capabilities, GuardKnox has earned Frost & Sullivan's 2018 Technology Innovation Award.

© Frost & Sullivan 2018

Significance of Technology Innovation

Ultimately, growth in any organization depends upon finding new ways to excite the market and upon maintaining a long-term commitment to innovation. At its core, technology innovation, or any other type of innovation, can only be sustained with leadership in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.

Understanding Technology Innovation

Technology innovation begins with a spark of creativity that is systematically pursued, developed, and commercialized. That spark can result from a successful partnership, a productive in-house innovation group, or a bright-minded individual. Regardless of the source, the success of any new technology is ultimately determined by its innovativeness and its impact on the business as a whole.

Key Benchmarking Criteria

For the Technology Innovation Award, Frost & Sullivan analysts independently evaluated two key factors—Technology Attributes and Future Business Value—according to the criteria identified below.

Technology Attributes

Criterion 1: Industry Impact
Criterion 2: Product Impact
Criterion 3: Scalability
Criterion 4: Visionary Innovation
Criterion 5: Application Diversity

Future Business Value

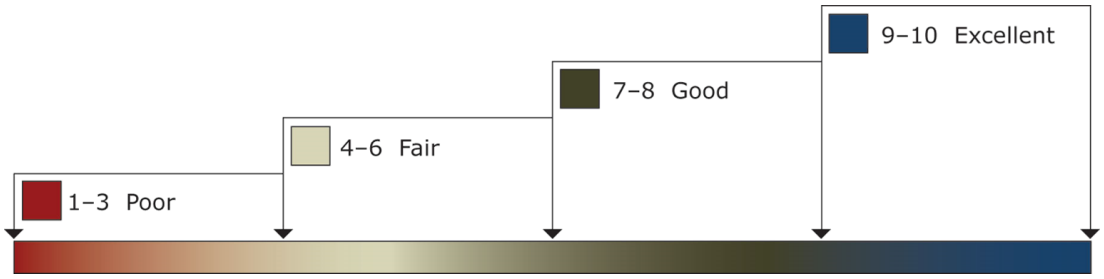
Criterion 1: Financial Performance
Criterion 2: Customer Acquisition
Criterion 3: Technology Licensing
Criterion 4: Brand Loyalty
Criterion 5: Human Capital

Best Practices Award Analysis for GuardKnox

Decision Support Scorecard

To support its evaluation of best practices across multiple business performance categories, Frost & Sullivan employs a customized Decision Support Scorecard. This tool allows our research and consulting teams to objectively analyze performance, according to the key benchmarking criteria listed in the previous section, and to assign ratings on that basis. The tool follows a 10-point scale that allows for nuances in performance evaluation. Ratings guidelines are illustrated below.

RATINGS GUIDELINES



The Decision Support Scorecard is organized by Technology Attributes and Future Business Value (i.e., These are the overarching categories for all 10 benchmarking criteria; the definitions for each criterion are provided beneath the scorecard.). The research team confirms the veracity of this weighted scorecard through sensitivity analysis, which confirms that small changes to the ratings for a specific criterion do not lead to a significant change in the overall relative rankings of the companies.

The results of this analysis are shown below. To remain unbiased and to protect the interests of all organizations reviewed, we have chosen to refer to the other key participants as Competitor 2 and Competitor 3.

Measurement of 1–10 (1 = poor; 10 = excellent)			
Technology Innovation	Technology Attributes	Future Business Value	**Average Rating**
GuardKnox	**8.0**	**7.5**	**7.8**
Competitor 1	6.8	7.2	7.0
Competitor 2	7.0	6.5	6.8

Technology Attributes

Criterion 1: Industry Impact

Requirement: Technology enables the pursuit of groundbreaking ideas, contributing to the betterment of the entire industry.

Criterion 2: Product Impact

Requirement: Specific technology helps enhance features and functionalities of the entire product line for the company.

Criterion 3: Scalability

Requirement: Technology is scalable, enabling new generations of products over time, with increasing levels of quality and functionality.

Criterion 4: Visionary Innovation

Requirement: Specific new technology represents true innovation based on a deep understanding of future needs and applications.

Criterion 5: Application Diversity

Requirement: New technology serves multiple products, multiple applications, and multiple user environments.

Future Business Value

Criterion 1: Financial Performance

Requirement: Potential is high for strong financial performance in terms of revenues, operating margins, and other relevant financial metrics.

Criterion 2: Customer Acquisition

Requirement: Specific technology enables acquisition of new customers, even as it enhances value to current customers.

Criterion 3: Technology Licensing

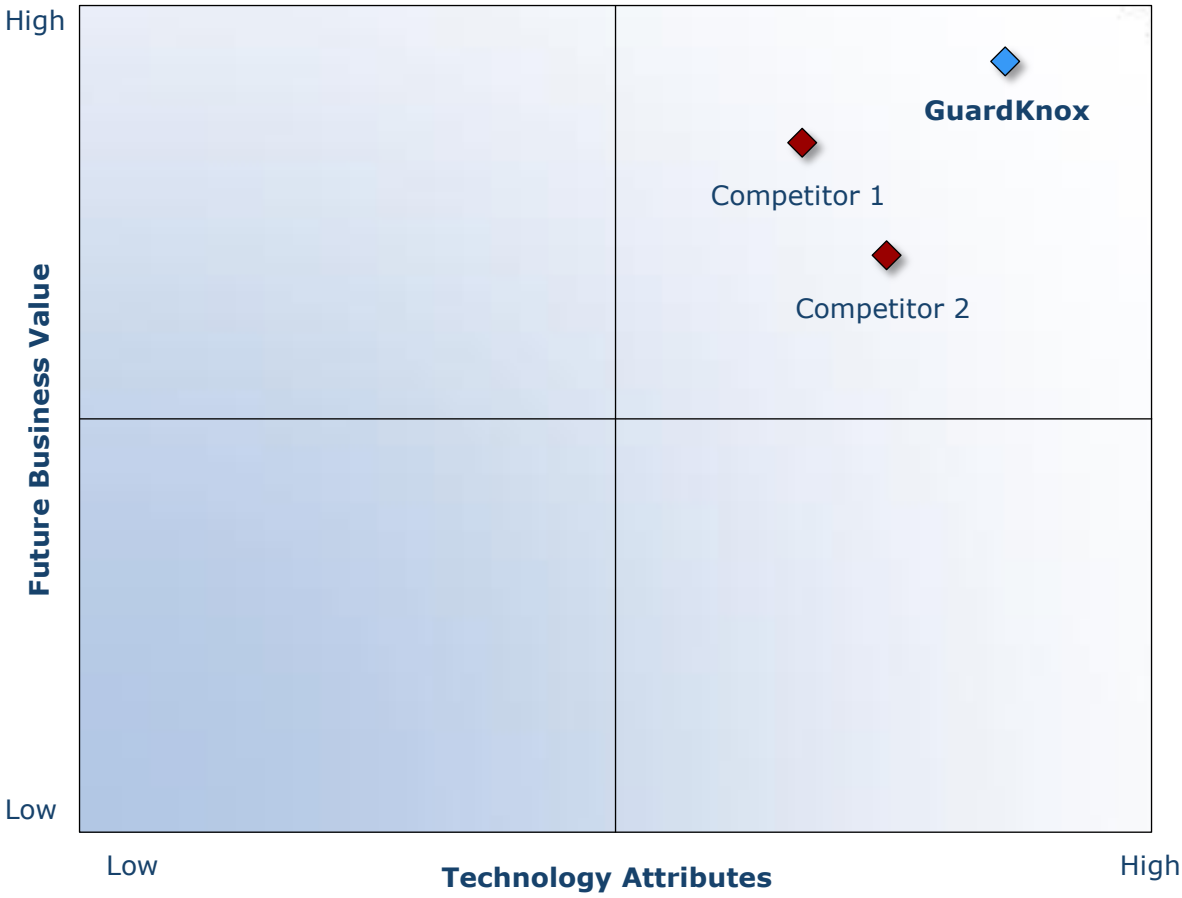
Requirement: New technology displays great potential to be licensed across many sectors and applications, thereby driving incremental revenue streams.

Criterion 4: Brand Loyalty
Requirement: New technology enhances the company's brand, creating and/or nurturing brand loyalty.

Criterion 5: Human Capital
Requirement: Customer impact is enhanced through the leverage of specific technology, translating into positive impact on employee morale and retention.

Decision Support Matrix

Once all companies have been evaluated according to the Decision Support Scorecard, analysts then position the candidates on the matrix shown below, enabling them to visualize which companies are truly breakthrough and which ones are not yet operating at best-in-class levels.



Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan analyst follow a 10-step process to evaluate Award candidates and assess their fit with select best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

	STEP	OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify Award recipient candidates from around the globe	• Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies	Pipeline of candidates who potentially meet all best-practice criteria
2	**Perform 360-degree research**	Perform comprehensive, 360-degree research on all candidates in the pipeline	• Interview thought leaders and industry practitioners • Assess candidates' fit with best-practice criteria • Rank all candidates	Matrix positioning of all candidates' performance relative to one another
3	**Invite thought leadership in best practices**	Perform in-depth examination of all candidates	• Confirm best-practice criteria • Examine eligibility of all candidates • Identify any information gaps	Detailed profiles of all ranked candidates
4	**Initiate research director review**	Conduct an unbiased evaluation of all candidate profiles	• Brainstorm ranking options • Invite multiple perspectives on candidates' performance • Update candidate profiles	Final prioritization of all eligible candidates and companion best-practice positioning paper
5	**Assemble panel of industry experts**	Present findings to an expert panel of industry thought leaders	• Share findings • Strengthen cases for candidate eligibility • Prioritize candidates	Refined list of prioritized Award candidates
6	**Conduct global industry review**	Build consensus on Award candidates' eligibility	• Hold global team meeting to review all candidates • Pressure-test fit with criteria • Confirm inclusion of all eligible candidates	Final list of eligible Award candidates, representing success stories worldwide
7	**Perform quality check**	Develop official Award consideration materials	• Perform final performance benchmarking activities • Write nominations • Perform quality review	High-quality, accurate, and creative presentation of nominees' successes
8	**Reconnect with panel of industry experts**	Finalize the selection of the best-practice Award recipient	• Review analysis with panel • Build consensus • Select recipient	Decision on which company performs best against all best-practice criteria
9	**Communicate recognition**	Inform Award recipient of Award recognition	• Present Award to the CEO • Inspire the organization for continued success • Celebrate the recipient's performance	Announcement of Award and plan for how recipient can use the Award to enhance the brand
10	**Take strategic action**	Upon licensing, company is able to share Award news with stakeholders and customers	• Coordinate media outreach • Design a marketing plan • Assess Award's role in future strategic planning	Widespread awareness of recipient's Award status among investors, media personnel, and employees

© Frost & Sullivan 2018

The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry participants and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages more than 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.