FROST & SULLIVAN

BEST PRACTICES AWARDS

GuardKNOX

2020 GLOBAL AUTOMOTIVE CYBERSECURITY SOLUTIONS VISIONARY INNOVATION LEADERSHIP

Contents

Background and Company Performance

Industry Challenges

The automotive industry is enduring a massive disruption from emerging technologies that make the link between wireless and additional connectivity and autonomous vehicles vulnerable to cyber threats. Given the vast amounts of personal information gathered from individuals using devices that are connected internally and externally to the vehicle throughout the day, the risk of breaching internal systems and electronic computing units (ECUs) has become progressively easier over the years for hackers. Moreover, so has the risk of using such a vulnerability to penetrate safety-critical systems such as the engine or the braking systems. Globally, Frost & Sullivan's research shows that the prevalence and sophistication of connected cars are rising and generating digitization and personalization trends at higher capacities more than ever when it comes to the level of connectivity and new system integrations. The automotive industry will see 850 million smartphone apps integration software units in-use by 2025; with original equipment manufacturers (OEMs) rapidly integrating features such as E-commerce marketplaces, on-demand services, third-party app stores, Vehicle-to-Everything wireless communication connectivity, in-Vehicle payable systems, digital assistants such as Amazon's ALEXA, and automotive biometrics.[1] With the various levels of end-to-end solutions available, the chances of personal data and private information getting into the wrong hands are increasing—leading to an evolving threat landscape; additionally, OEMs seek cost-effective automotive cybersecurity solutions for building into vehicles.

Interconnecting network operating systems and establishing a secure connection between multiple networks is an ideal consideration for OEMs to address during the integration process. The complexity of interconnecting network operating systems in modern vehicles makes it challenging for OEMs to establish a secure connection between various networks in addition to meeting different verification protocols and security standards. Furthermore, with the current market trends and the evolving paradigm shift, OEMs are searching for an appropriate way to safely parallel the smartphone revolution to the automotive revolution.

Deterring the advantages of cyber-attacks is challenging, given that the automotive supply chain remains heavily dispersed when it comes to its value chain; furthermore, offering a cyber-security solution that can detect all attack levels of cyber threats is difficult. With the popularity and level of in-vehicle connectivity rising, changing market trends leading the pace, the landscape, and usage in regards to external devices increase as well. Frost & Sullivan notes that as external devices multiply, connectivity with external devices uncover threat vectors and increases product vulnerability, which in turn exposes vehicles and sensitive data that include personal information and location points. The popularity of electric vehicles (EV) is a prominent example of the challenge for increasing cyber threat awareness. The commercial public EV charging ecosystems face numerous potential cyber and EV charging threats, gaining access to various end-points such as

[1] *Global Connected Car Market Outlook, 2019* (Frost & Sullivan, March 2019)

charging system hardware or physical interfaces (including USB ports), charging system software, and physical or wireless communication links.[2]

Lastly, cybersecurity solutions must remain robust, standalone, and device-agnostic when it comes to communication capabilities, especially in an industry as fragmented as automotive. With the state of vulnerability increasing for connected vehicles, the need for solutions to offer top security performance is essential in deterring all types of threat scenarios and, at the same time, enable seamless integration. Frost & Sullivan identifies a key challenge as orchestrating secure connectivity between two different internal networking channels in a vehicle when establishing network operations inside modern cars. To develop top-level security, cybersecurity solutions and services must accommodate the need for real-time personalization and customization (layering top-level security and optimal service) when it comes to maintaining a positive end-user experience and the entire lifespan of connected vehicles. Cybersecurity should be viewed as a necessity and as a foundational layer all throughout the multitude of design phases in vehicle production in order to securely and safely enable additional levels of connectivity.

Focus on the Future and Best Practices Implementation of GuardKnox

Founded in 2016, an Israel-based automotive technology company, GuardKnox Cyber Technologies (GuardKnox), delivers comprehensive cybersecurity computing platforms and added services (application downloads and vehicle customization) for the automotive industry. The GuardKnox team brings decades of experience providing similar solutions to the critical assets of the state of Israel, including the Iron Dome, Arrow III, and F-35 fighter jet. This includes invaluable expert knowledge in defending embedded, safety-critical systems where lives are on the line in moving platforms. The unique and patented methodologies are geared specifically for the automotive systems with an automotive price tag.

In 2018, Frost & Sullivan recognized GuardKnox for its technology innovation leadership attributes stemming from its comprehensive hardware and software solutions that seamlessly integrate into the vehicle, the value chain, and the vehicle production process. The company also has a designated product line for aftermarket and retrofitting applications. Currently, the company is in various stages of the RFP/RFQ stage with prominent OEMs and Tier 1 companies with various executed commercial agreements. GuardKnox plans to continue developing high-performance, consolidated, flexible, and scalable computing platforms for current and next generation of vehicles alongside strategic industry veterans and partners.

In June of 2019, GuardKnox gained strong support from the French global automotive supplier, Faurecia as well as a number of global players including but not limited to Fraser McCombs Capital, Shanghai Automotive Industry Corporation (SAIC), Plug and Play, NextLeap VenturesGlory Ventures, the Livnat Family, Allied, Kardan.[3] In addition to these corporations, GuardKnox also received investment from a group of esteemed European

[2] https://blog.guardknox.com/ev-charging-threats-cybersecurity-ev-charging-ecosystem

[3] https://www.calcalistech.com/ctech/articles/0,7340,L-3771405,00.html

executives, including Dr. Paul Achleitner, Dr. Juergen Hambrecht, Dr. Kurt Lauk, Prof. Dr. Roland Berger, Michael Diekmann, and Peter Loescher among others who invested in their own personal and private capacity. In doing so, Frost & Sullivan firmly believes GuardKnox will drive its leadership beyond the European region, increasing its global presence and footprint even further around the world.

Taking Visionary Strides towards Market Leadership

GuardKnox's offerings stem from its Secure Network Orchestrator platform, serving as a secure and optimized vehicle ECU or domain controller that, in turn, delivers the foundation for both current and future personalization and customization of vehicles. The foundation consists of an in-depth security approach being built from the ground up. The patented Lockdown™ core parses all vehicle communications in real-time to ensure a completely deterministic solution that upholds the highest level of safety and security for all those on the road. The patented Service-Oriented Architecture (SOA) establishes a unified communication, in addition to access control and service level partitioning to create a secure environment for application and data hosting, storage, and processing. The patented technologies provide an optimized and unique approach to the needs of the automotive industry, including high-performance computing platforms and a consolidated approach that enables long term cost savings and open doors to new revenue streams.

Through a joint solution offering with Palo Alto Networks, GuardKnox is able to offer a true end-to-end solution that enables a variety of new services that depends on the secured transmission of information between service providers or operational centers and the vehicles. The solution empowers OEM vendors to secure over-the-air (OTA) communication between the vehicle, the cloud, and their operation centers with the GuardKnox platform as the secured in-vehicle landing point for updates, upgrades, customization and much more. Furthermore, the strategic partnership with DXC Technology enables data transmission to the DXC Security Operations Center (SOC) with real-time monitoring and in-depth analysis of security-related events. SOC analysts are presented with well defined, targeted, and actionable intelligence enabling them to ascertain which vehicles were under attack along with the purpose and method of the attack.

However, GuardKnox's solutions offer more than just end-to-end holistic solutions. As a unique value proposition to its customers, the company can provide the highest level of security to the automotive industry through its patented Communication Lockdown™ Methodology (USPTO 9,899,563 B2). Furthermore, the patented architecture creates a consolidated and cost-effective platform that is being used for the current and next generation of vehicles by supporting the computing power and performance needed to support additional levels of connectivity securely. OEMs can not only provide customers with a secure communications channel but also with reusable code components that decrease deployment time; pass along data regardless of language origin; scalability; and reduced costs—these benefits allow OEMs to monetize throughout a vehicle's life cycle.[4]

[4] https://www.guardknox.com/services-oriented-architecture-automotive-services/

Lastly, Communication Lockdown™ Methodology also provides robust, verifiable, and efficient attack resistance capabilities, unlike competitor's solutions in the market that are heavily based off of IT-based or learning solutions that require constant connectivity, networking scanning, machine learning and much more. Communication Lockdown Methodology™ utilizes strict rule-sets that grant only authorized information and communication.

GuardKnox enhances the security levels needed in the infrastructure of connected vehicles by creating a standalone domain controller or gateway unit that not only offers security layering but provides real-time customization for the vehicle's entire lifespan. In other words, GuardKnox completely eliminates vulnerabilities, allowing the opportunity for end-users to adhere to various levels of cyber-attacks and adapt to new system requirements over time.

Strategic Investments and Relationships for Future Growth

GuardKnox's vision for excellence is possible from its relationships with key investors, both private and corporate, to turn its cybersecurity solutions into a reality, in addition to positioning the company for long-term growth and stability. The illustrious investor portfolio spans across all corners of the globe positions GuardKnox to have and maintain a global footprint and better serve the respective markets. The investor partnerships allow GuardKnox to further its visionary drive and ability to deliver outstanding solutions within the automotive market. Alongside these partnerships, GuardKnox raised $21 million in capital investment in 2019 upon funding completion. Plans are underway to expand subsidiaries and its internal research and development teams globally. Most recently, the company increased its reach globally with new subsidiaries in Stuttgart, Germany, and Detroit, Michigan, in the United States. GuardKnox continues to explore other regions such as the Asia-Pacific with endeavors to reach China and Japan.

Frost & Sullivan recognizes the strategic commitment of the company's focus on the future and the powerful impact its solutions can potentially have on the automotive market. Demonstrating a robust and out-of-the-box approach that leverages the company's many successful partnerships, GuardKnox is capable of offering superior solutions for automotive manufacturers that cater to end-users and its customer base. In doing so, the influence of the company's patented comprehensive hardware and software in-vehicle solutions, such as Communication Lockdown™ Methodology and SOA, allows for simple integration in the aftermarket or during the production process. Due to the high-performance and computing capabilities, secure software firmware and hardware upgrades are enabled over-the-air, thus eliminating the need for extra costly hardware. As the company maintains continuous patents for its SOA structures, GuardKnox is uniquely positioned to reach industry leadership. With strategic plans for the future, the company strives to assist Tier 1 suppliers and OEMs by generating additional revenue streams and decreasing overall lifecycle costs through its patented in-vehicle solutions and its clear opportunistic vision of a personalized, safe and secure, and upgraded driving experience for the automotive industry.

Conclusion

The future of automotive connectivity infrastructures continues to flourish as consumers adopt higher levels of enhanced system integration and capabilities. However, connected vehicles continue to remain a target for serious cyber threats. Because of the critical impact of cyber-attacks, customers require solutions that can offer a more robust level of protection and deliver future personalization and customization over a vehicle's lifespan, protecting the vehicles of today and tomorrow.

GuardKnox leverages its innovative cybersecurity hardware and solutions to address the needs of the automotive industry while at the same time continuing to enhance the market with its visionary attributes. Frost & Sullivan recognizes GuardKnox for its ideal approach towards optimizing automotive cybersecurity, with future strides to empower original equipment manufacturers (OEMs) to create top-tier security-empowered vehicles.

With its strong overall performance and future strides for automotive connectivity protection, GuardKnox earns Frost & Sullivan's 2020 Global Visionary Innovation Leadership Award for the automotive cybersecurity solutions market.

Significance of Visionary Innovation Leadership

A Visionary Innovation Leadership position enables a market participant to deliver highly competitive products and solutions that transform the way individuals and businesses perform their daily activities. Such products and solutions set new, long-lasting trends in how technologies are deployed and consumed by businesses and end users. Most important, they deliver unique and differentiated benefits that can greatly improve business performance as well as individuals' work and personal lives. These improvements are measured by customer demand, brand strength, and competitive positioning.

Understanding Visionary Innovation Leadership

Visionary Innovation is the ability to innovate today in the light of perceived changes and opportunities that will arise from Mega Trends in the future. It is the ability to scout and detect unmet (and as yet undefined) needs and proactively address them with disruptive solutions that cater to new and unique customers, lifestyles, technologies, and markets. At the heart of visionary innovation is a deep understanding of the implications and global

ramifications of Mega Trends, leading to correct identification and ultimate capture of niche and white-space market opportunities in the future.

Key Benchmarking Criteria

For the Visionary Innovation Leadership Award, Frost & Sullivan analysts independently evaluated two key factors—Focus on the Future and Best Practices Implementation—according to the criteria identified below.

Focus on the Future

Criterion 1: Focus on Unmet Needs
Criterion 2: Visionary Scenarios through Mega Trends
Criterion 3: Growth Pipeline
Criterion 4: Blue Ocean Strategy
Criterion 5: Growth Performance

Best Practices Implementation

Criterion 1: Vision Alignment
Criterion 2: Process Design
Criterion 3: Operational Efficiency
Criterion 4: Technological Sophistication
Criterion 5: Company Culture

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

Frost & Sullivan Awards 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

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 players 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.