Cybellum Recognized as the

2021

Company of the Year

European Vehicle Security and Risk Assessment Industry

Excellence in Best Practices

FROST & SULLIVAN

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Cybellum excels in many of the criteria in the in-vehicle security and risk assessment space.

Addressing Unmet Needs & Leadership Focus

Digital transformation is disrupting the automotive industry, with the rise in connected vehicles exposing automobiles to new cybersecurity attacks. Addressing automotive cybersecurity is crucial as software vulnerabilities in connected vehicles can threaten customers' lives and tamper with their data privacy. Moreover, such risks invariably tarnish the brand reputation of OEMs and have a catastrophic effect on customer confidence and safety. Connected cars' security can be compromised due to a range of vulnerabilities, including weaknesses in mobile apps, misuse of personal data, backend server hacks, and remote hacking of keyless vehicle systems. Connected cars collect up to 25 gigabytes of personal data every hour and recent analysis from Uswitch indicates vehicle cyberattacks have increased by 99% since 2020[1]. As a result, automakers are seeking partners who can help automakers mitigate security issues beginning at the design concept stage through the vehicle ownership lifecycle.

[1] https://www.am-online.com/news/manufacturer/2020/06/04/cyber-attacks-on-connected-cars-rise-by-99

Founded in 2016 and is headquartered in Tel Aviv, Israel, Cybellum is an automotive cybersecurity company empowering automotive original equipment manufacturers (OEMs) and suppliers to identify and remediate security risks. The company's solutions work at scale and throughout the entire vehicle life cycle.

To combat the aforementioned challenges, the company has launched the Cybellum Cyber Digital Twins™ platform. It exposes the underlying S-BOM, hardware architectures, operating systems,

configurations, control flows, API calls, licenses, encryption algorithms and keys, hardening mechanisms and more – generating an accurate digital replica - a Cyber Digital Twin - of every vehicle component in the backend server, subsequently the platform runs threat analysis and monitoring solutions to detect and remediate potential vulnerabilities. While the digital twin concept has been around for quite some time, Cybellum's platform uniquely allows automakers to continuously detect, identify, and trace potential cyber vulnerabilities in each vehicle component. Through contextual analysis of vulnerabilities, the Cyber Digital Twins platform will automatically prioritize the most relevant and pressing security issues and will generate remediation procedures to help automakers overcome threats. The digital replica remains in the service of the automotive company even after the vehicle has left the factory, enabling continuous threat monitoring, proactive risk identification and incident response throughout a vehicle's lifespan.

Cybellum's world-class vehicle security and risk assessment solution has come at a fortuitous time (i.e., when the automotive industry has tightened regulations for manufacturers to ensure vehicle safety and security). The company's Cyber Digital Twins platform is considered a revolution in automotive cybersecurity as it provides manufacturers the infrastructure to develop and maintain secure products at scale. It enables the continuous security assessment and monitoring of a product from its design, launch and on-going use, ensuring full control and governance throughout the product lifecycle.

The Cyber Digital Twins platform utilizes two key solutions to manage threats during the design and development and vehicle operation phases, namely:

- ***Product Security Assessment.*** Cybellum's Product Security Assessment solution was built for automotive product security teams enabling them to perform security analysis and compliance validation before the start of production, based on the Cyber Digital Twin of each component. The Product Security Assessment solution efficiently identifies security gaps, including common vulnerabilities and exposures, zero-days, hardening issues, and cryptography violations in the software and companion mobile apps. It continuously tracks and filters out irrelevant vulnerabilities while prioritizing the risks that matter the most. The solution subsequently eliminates vulnerabilities through remediation guidelines. To support continuous security validation from design to production, it integrates with manufacturer's product management systems such as ALM and PLM and with CI/CD systems and tools, creating a seamless DevSecOps process.
- ***Product Security Operations***. Cybellum's Product Security Operations solution automates vehicle security monitoring, without requiring an embedded code in the vehicle component. It continuously tracks new and existing vulnerabilities and security threats, evaluate their impact on operational components and vehicles, facilitated root-cause analysis and launch incident response plans quickly to minimize automakers' liability while safeguarding vehicles and passengers. To quickly and efficiently close the security loop, Cybellum's Product Security Operations solution integrates with SIEM, OTA and VSOC systems.

Overall, the Cyber Digital Twins platform offers a comprehensive, end-to-end cybersecurity management platform for automakers. Even after a vehicle has left the assembly line, manufacturers can use Cybellum to monitor their security posture, identify potential risks, and fix them before any

damage is done. The solution also helps users seamlessly comply with upcoming stringent security regulations and standards, internal security policies and OSS licensing guidelines for every component developed inhouse or by suppliers.

Cybellum is a market leader due to its unique ability to expose not just the vulnerability, but also the entire attack chain. Consequently, OEMs and their suppliers have a clear picture of the potential damage such risks pose. Frost & Sullivan believes Cybellum is favorably positioned to win trust among automakers due to its ability to manage risks throughout the product lifecycle. Moreover, its backend and offboard approach makes Cybellum more reliable and process-efficient than competitors.

Best Practices Implementation

By 2022, cybersecurity standards (i.e., ISO 21434 and UNEC WP29 (WP.29) will be published and mandated in certain countries. ISO 21434 prioritizes vehicle security-by-design while UNEC WP.29 aims to secure vehicles from development to the post-production stage through the deployment of efficient cybersecurity management systems (CSMS). Considering these standards, OEMs will be mandated to build a risk-based assessment framework to continuously monitor and ensure vehicle systems, software updates, security operations centres (SOC), and CSMS remain compliant with regulations. The need to perform regular certification checks, pressurized deadlines, and limited auditing budgets make many OEMs third-party dependent. Approximately 50 to 60% of OEMs prefer to work with third-party companies to set up SOCs, CSMS, and auditing services.

The Cybellum Cyber Digital Twins platform enables automakers to adhere to threat management requirements set by regulations such as UNECE WP.29 and ISO/SAE 21434. To that end, a digital twin for each vehicle component is created in the backend and checked for potential vulnerabilities. A threat exploitability and severity-level analysis is also performed. As a result, the offering provides a full impact assessment on automakers' entire vehicle fleets while providing the necessary mitigation measures. Such an offboard and agentless approach allows automakers to seamlessly identify and mitigate threats mentioned in the regulatory documents, helping them remain compliant.

Cybellum's differentiated ability to manage security threats throughout the vehicle ownership lifecycle (from the design phase through deployment and policy imposition) helps automakers meet regulations favorably, positions it over competitors. As a result, it is successfully winning deals with automotive OEMs.

Brand Equity

Cybellum is a market leader in the vehicle security and risk assessment industry and has already partnered with ten manufacturers and suppliers across the United States, Europe, Japan, and China. The company's extensive cybersecurity and defense knowledge help it approach vehicle security challenges in a uniquely effective manner. Such an approach is a key success pillar for Cybellum. The company plans to continue expanding its market presence to support other industries facing similar security challenges underlying embedded components, such as the Industrial Internet of Things and medical devices.

Cybellum's unique automotive cyber risk assessment technology and customer and partner engagements have paved the way for funding. In 2020, Cybellum raised $12 million in a funding round

led by RSBG Ventures GmbH, with additional investment from Blumberg Capital and Target Global. The round A funding brings the total investment in the company to $15 million. The capital fund will allow Cybellum to accelerate its growth, expand its market presence, and increase penetration of Cybellum's Cyber Digital Twin platform across more industries. It will hence be able to scale vulnerability management operations.

Customer Purchase and Service Experience

The automotive industry has a highly complex supply chain. Manufacturers rely on hundreds of independent vendors for their internal hardware and software components and this complex structure is fraught with vulnerabilities and security threats. Hence, extensive validation testing from the automaker's end. The biggest challenge is identifying whether suppliers have built adequate cybersecurity into their components. The result of a recent survey conducted by SAE International showed that only 19% of respondents perform ample security testing during the requirements and design phase. 28% of respondents said exhaustive testing was done only in the development and testing phase, which is far too late. Other suppliers only perform security testing of their components post-release, significantly increasing remediation costs. To get better results, automakers and suppliers must improve cybersecurity testing and vulnerability management early.

Cybellum's automotive risk assessment solutions improve supply chain security by ensuring every single component inside vehicles is meticulously inspected and found safe and secure. This is achieved with the help of Cybellum's revolutionary Cyber Digital Twins platform and security assessment technology, together which expose all the software vulnerabilities in each of the vehicle's components through binary code analysis (without requiring their source code). The Cyber Digital Twins platform screens every aspect of the code - be it open-source, commercial or proprietary code - for potential vulnerabilities and risk exposure, allowing manufacturers to act immediately and eliminate any cyber risk before harm is done.

The Cyber Digital Twins platform replicates even the smallest details of each software component needed for security analysis, subsequently scanning for new and emerging vulnerabilities and identifying potential threats that impact certain makes, models, and manufacturing series. Automotive security teams can thus ensure the cars are well protected, irrespective of the make and model or how long it has been on the road. Cybellum's solutions prioritize the vulnerabilities based on the severity and risk they pose to the specific makeup and composition of the vehicle's critical systems. In 2020, Cybellum partnered with the Tel Aviv-based innovation lab of the Renault–Nissan–Mitsubishi Alliance Group to develop cybersecurity technologies and a risk-based threat assessment framework. The Cybellum Cyber Digital Twins platform identifies a wide range of vulnerabilities in the electronic control units, gateways, communication networks, and software inside the vehicles to provide necessary incident response plans. The Alliance Group utilizes the Cybellum solution suite to gain end-to-end visibility of potential threats within their vehicle components, receiving the necessary guidance on risk remediation procedures, and preparing for upcoming security regulations, all of which provide a competitive edge. Chris Dickman, the global chief of cybersecurity services and research for Nissan Motors stated Cybellum helped to reduce their mean time to detect (MTTD) by 80%, allowing the company to automatically

identify known and unknown vulnerabilities with limited human intervention. Cybellum also lists Jaguar-Land Rover, Harman, CATARC and GIGA amongst its customers.

In 2021, Cybellum partnered with PTC to integrate its solution into PTC's Windchill RV&S, a systems and software engineering solution geared toward manufacturers. The joint security solution performs automated security scanning on top of Windchill RV&S PLM system to achieve compliance with all required safety and security regulations. Even though the software source code and built executables are managed within Windchill RV&S, Cybellum's Cyber Digital Twins conducts cybersecurity evaluations on the binary code, making sure each component is tested for its cybersecurity score. Manufacturers can now define software security considerations early in the product life cycle and alongside the product engineering process and manage the entire product's cybersecurity risks. The software developers can also proactively test and fix identified security threats using automatically generated and detailed remediation procedures. The joint solution helps manufacturers adopt a Security-by-Design approach and comply with cybersecurity regulations such as ISO 26262 (road vehicles functional safety), UNECE WP.29 (the world forum for the harmonization of vehicle regulation), and ISO 21434 (DIS road vehicles cybersecurity engineering).

Cybellum focuses on the highest levels of vehicle security and is deeply committed to engaging customers in new experiences through its technology. Unlike its competitors, Cybellum manages security gaps throughout the entire product life cycle, assuring an outstanding customer experience. The company's comprehensive threat detection and Cyber Digital Twin platform approach uniquely position Cybellum to help automotive clients secure their massive fleets of connected vehicles from current and future cyberattacks.

Conclusion

Effective cybersecurity management for the automotive sector includes supply chain visibility, adherence to upcoming regulations, detailed vulnerability assessment, and quick time to response. Cybellum's revolutionary Cyber Digital Twins offering provides automatic threat monitoring and risk assessment through an offboard agentless and backend approach. It uniquely performs security analysis on the digital replica of each vehicle component without accessing the source code while eliminating the need for power-consuming security solutions to be implemented inside vehicles. As a result, Cybellum helps clients seamlessly adopt Security-by-Design and achieve regulatory compliance quickly and cost-effectively.

For its exceptional performance, product value, and outstanding customer support, Cybellum earns Frost & Sullivan's 2021 Company of the Year Award in the European vehicle security and risk assessment industry.

What You Need to Know about the Company of the Year Recognition

Frost & Sullivan's Company of the Year Award is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Award Analysis

For the Company of the Year Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Visionary Innovation & Performance

Addressing Unmet Needs: Customers' unmet or under-served needs are unearthed and addressed by a robust solution development process

Visionary Scenarios Through Mega Trends: Long-range, macro-level scenarios are incorporated into the innovation strategy through the use of Mega Trends, thereby enabling first to market solutions and new growth opportunities

Leadership Focus: Company focuses on building a leadership position in core markets and on creating stiff barriers to entry for new competitors

Best Practices Implementation: Best-in-class implementation is characterized by processes, tools, or activities that generate a consistent and repeatable level of success

Financial Performance: Strong overall business performance is achieved in terms of revenue, revenue growth, operating margin, and other key financial metrics

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

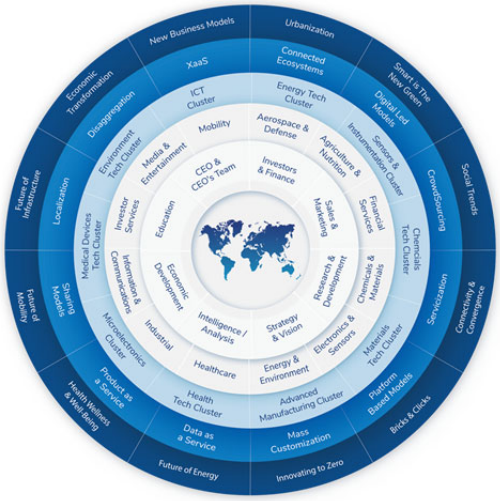
Frost & Sullivan's proprietary model to systematically create on-going growth opportunities and strategies for our clients is fuelled by the Innovation Generator™. Learn more.

Key Impacts:

- **Growth Pipeline:** *Continuous flow of Growth opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our six analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.



Analytical Perspectives:

- Mega Trend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)