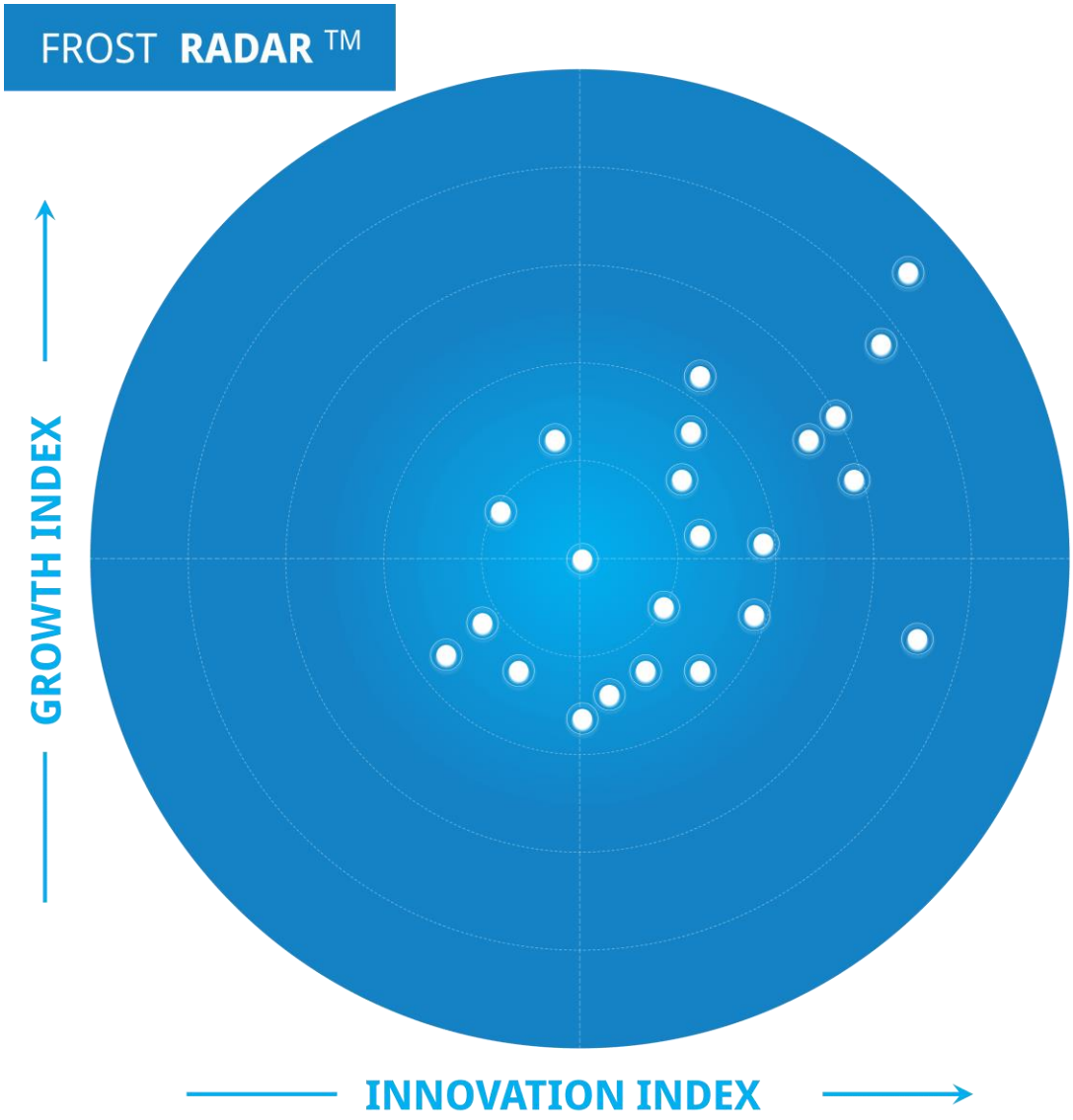
Frost Radar™

Automotive Cybersecurity, 2024

A Benchmarking System to Spark Companies to Action - Innovation that Fuels New Deal Flow and Growth Pipelines

Authored by
Dorothy Amy

With contributions by
Thanigesh Parthasarathi



PF9E-42
May 2024

Research Summary

This Frost Radar™ highlights 7 leading companies in the automotive cybersecurity sector that are actively engaged in advancing cybersecurity solutions for original equipment manufacturers (OEMs) and Tier 1 suppliers in the automotive industry.

The Radar assesses the key cybersecurity specialist companies such as PlaxidityX (formerly Argus Cyber Security Ltd.), Upstream Security, Karamba Security Ltd, AUTOCRYPT, Cybellum Technologies LTD, VicOne, and ETAS GmbH, all dedicated to addressing the unique cybersecurity challenges faced by the automotive sector.

This Radar evaluates these vendors based on their Innovation and Growth indices, illustrating their market strength. It provides an overview of each company's cybersecurity offerings, research and development (R&D) endeavors, revenue trajectory, investment activities, client base, and future strategies. Additionally, this analysis delves into the specific cybersecurity technologies embraced by each vendor and the rationale behind their adoption within the automotive cybersecurity landscape.

Through this Frost Radar™ analysis, industry stakeholders can gain valuable insights into the prevailing cybersecurity challenges within the automotive sector, anticipate shifts in business models, and identify critical capabilities to consider when collaborating with automotive cybersecurity vendors.

Frost & Sullivan analyzes numerous companies in an industry. Those selected for further analysis based on their leadership or other distinctions are benchmarked across 10 Growth and Innovation criteria to reveal their position on the Frost Radar™. The publication presents competitive profiles of each company on the Frost Radar™ considering their strengths and the opportunities that best fit those strengths.

Strategic Imperative

The automotive cybersecurity industry is gaining traction with the increased integration of digital technologies in vehicles. As vehicles become more connected and incorporate autonomous features, there is an urgent need to secure vehicle systems from cyber threats. The industry is characterized by the emergence of cybersecurity firms specializing in automotive security solutions and robust collaborations between traditional automotive manufacturers and technology companies.

AI-powered cybersecurity solutions are poised to revolutionize the automotive sector by enabling proactive threat detection, anomaly detection, and adaptive defense mechanisms. These advanced solutions will play a pivotal role in ensuring the resilience of automotive systems against evolving cyber threats.

As automotive manufacturers strive to integrate cutting-edge technologies such as autonomous driving, vehicle-to-grid (V2G) charging, vehicle-to-everything (V2X) communication, and over-the-air (OTA) updates, the need for powerful cybersecurity solutions will become more pronounced. Effective automotive cybersecurity solutions will not only mitigate the risk of cyberattacks, but also foster trust among consumers, encouraging the widespread adoption of next-generation connected and autonomous vehicle technologies.

This Frost Radar™ captures the pivotal shifts and technological advancements in the automotive cybersecurity industry and how stakeholders utilize them to fortify vehicle security amid evolving threats within the connected vehicle ecosystem.

The analysis includes vendor and technology assessments, partner and customer ecosystem, competitive index and regional footprint, and industry overview. The industry overview highlights the significance of automotive cybersecurity in fostering trust among consumers and stakeholders, facilitating the evolution of smart and connected vehicles, and ensuring passenger safety and integrity of the automotive ecosystem.

Growth Environment

The automotive cybersecurity industry is in an emerging growth phase and is poised for rapid expansion to mitigate the growing security and data privacy risks associated with the integration of digital technologies into vehicles. With the proliferation of connected cars and autonomous driving systems, ensuring cybersecurity has become a paramount concern for automakers and stakeholders across the value chain.

In-vehicle intrusion detection and prevention, threat assessment and vulnerability management, and cybersecurity management systems are among the key solutions in demand to adhere to regulatory compliance pressures for continuous threat monitoring throughout a vehicle's lifecycle.

Governments and regulatory bodies continuously enhance automotive cybersecurity standards and regulations to guide manufacturers in ensuring compliance. For instance, the United Nations Economic Commission for Europe (UNECE) WP.29 regulation mandates cybersecurity management systems for connected vehicles, driving automakers to prioritize cybersecurity measures in their product development and compliance strategies. The UNECE regulatory requirements (UN R155 and R156) apply in 54 member countries, including the European Union, the United Kingdom, Japan, and South Korea. Non-member countries are considering the implications of these regulations for enabling sales in member countries.

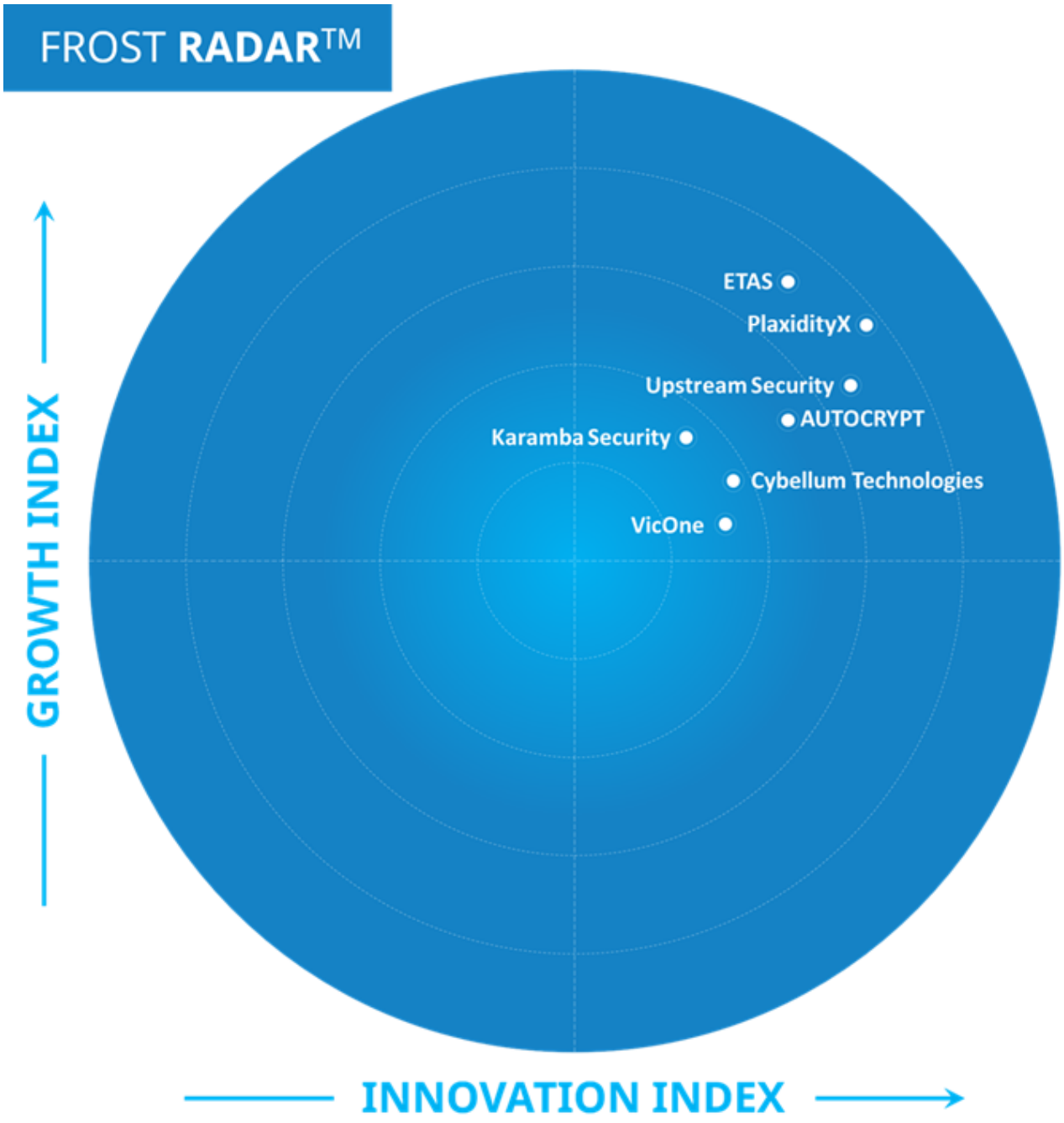
Collaboration between automakers, cybersecurity firms, and technology providers is increasingly prevalent as stakeholders recognize the collective effort required to address cybersecurity challenges effectively. Partnerships and alliances aim to nurture innovation, share best practices, and contribute to developing cutting-edge cybersecurity solutions tailored to the automotive ecosystem's unique requirements.

Advancements in technologies such as artificial intelligence (AI), machine learning (ML), and blockchain drive innovation in automotive cybersecurity. AI-powered threat detection algorithms, ML-based anomaly detection systems, and blockchain-enabled secure communication protocols are poised to revolutionize how automotive cybersecurity is approached, offering proactive defense mechanisms against evolving cyber threats.

Frost & Sullivan studies related to this independent analysis:

- Global Automotive Cybersecurity Growth Opportunities
- Global Quantum Computing Growth Opportunities

Frost Radar™



Source: Frost & Sullivan

Competitive Environment

In an industry of more than 20+ global participants, Frost & Sullivan has identified 7 potential cybersecurity companies disrupting the automotive industry: PlaxidityX (formerly Argus Cyber Security Ltd.), ETAS GmbH, Upstream Security, AUTOCRYPT, Cybellum Technologies LTD, Karamba Security Ltd, and VicOne.

Cybersecurity is a critical prerequisite in the automotive sector as vehicles become more connected. Automotive OEMs must comply with automotive cybersecurity regulatory standards, such as the UN R155 and ISO 21434, to obtain type approvals for vehicles such as motorcycles, scooters, electric bicycles, passenger cars, pickup trucks, commercial vehicles, and shared mobility fleets.

To address this pressing need to adhere to stricter security regulations, the automotive industry is witnessing an influx of technology companies embracing distinctive approaches to cybersecurity. Specialist cybersecurity vendors, technology companies with integrated cybersecurity divisions, and Tier 1 suppliers with internal cybersecurity teams compete in the space to innovate and offer better solutions.

PlaxidityX has secured the top position in the Innovation Index for its rich portfolio of cybersecurity solutions, including in-vehicle security products, aftermarket car theft protection solutions, vulnerability assessment, threat mitigation solutions, vehicle security testing, and compliance-related services. In addition to its comprehensive portfolio, the company has launched a new DevSecOps platform tailored specifically for automotive software development to facilitate end-to-end security measures for the entire software development process. PlaxidityX stands out for its ability to adapt to evolving regulations, which is evident from its stringent compliance services for the two-wheeler (2W) segment. PlaxidityX also ranked second in the Growth Index by exhibiting an impressive 500% revenue growth since 2021.

ETAS GmbH excels as the Growth leader in the Radar, recording the highest revenue relative to its competitors in 2023, signaling a robust growth trajectory. The company's vast presence across Europe, Asia, and the Americas solidifies its potential to acquire new clients across diverse regions.

Upstream Security secured the second-highest position on the Innovation Index, owing to its breakthrough cloud-enabled applications and enhanced solutions portfolio. The company differentiates itself through ongoing investments in a wide array of mobility-specific use cases and strategic partnerships to attract a larger audience in the automotive sector.

AUTOCRYPT is ranked third in the Innovation index for its efforts in developing dedicated V2X and electric vehicle charging security solutions, distinguishing it from the competition. Providing the industry’s only V2X security solution highlights its focus on defining the future of self-driving vehicles. The V2X solution works with multiple V2G root environments, resolving a long-standing compatibility issue for service providers with different car models. The company has a total of 37 vehicle security-related projects to date, contributing to its strong revenue performance.

Karamba’s competitive positioning in the Growth index is primarily attributed to its impressive client list and security engagements in the automotive industry. Through its engagements with Fortune 500 companies, Karamba has secured a fleet of 800,000 units in over 100 countries.

Cybellum and VicOne occupy the next 2 spots after AUTOCRYPT in the Innovation Index. Cybellum’s powerful product security platform, visionary partnerships with automotive stakeholders, and strong clientele showcase its effective growth strategy.

However, its narrow product portfolio limits its position in the Innovation index. VicOne has extended its solution to electric buses through a recent partnership with Clientron; however, its primary focus on the Asia-Pacific region limits its position in the Growth index.

Note: C2A Security was considered for inclusion, but a product direction change in the last 2 years meant that an objective comparison was not possible.

PlaxidityX (formerly Argus Cyber Security Ltd.)

Innovation

- PlaxidityX (formerly Argus Cyber Security Ltd.) takes a holistic approach to automotive cybersecurity to help OEMs and suppliers secure vehicle components, networks, and fleets and ensure compliance with industry regulations. Its diverse range of products and services includes in-vehicle security, vulnerability assessment, threat mitigation, vehicle security testing, and compliance-related solutions.
- PlaxidityX holds more than 100 granted and pending automotive cybersecurity patents, demonstrating the scalability of its proprietary solutions suite in addressing various cybersecurity vulnerabilities in the automotive industry.
- The company partners with tech leaders such as Microsoft, AWS, Google, Eviden, Checkpoint Software, and IBM to enhance the capabilities of its cybersecurity solutions.
- Collaborations with dSPACE, Elektrobit, and Amazon's Alexa highlight Argus's innovative approach to leveraging partnerships for enhancing its cybersecurity solutions' capabilities, whether through streamlining development processes or integrating with popular voice assistant platforms.
- PlaxidityX vDome is a unique cybersecurity product that protects new and used vehicles from theft and fraudulent activities. vDome proactively detects malicious devices in under 200 microseconds. It identifies all ECUs on the CAN bus and creates a unique electrical signature for each ECU signal, which represents a distinct “fingerprint” that cannot be faked, thereby providing the highest level of security for vehicles on the road.
- In 2024, PlaxidityX unveiled a new DevSecOps platform tailored specifically for automotive software development. Designed for OEMs and Tier 1 suppliers, this platform facilitates the seamless integration of security measures throughout all stages of the software development process. Doing so enables automotive manufacturers to expedite their time to market and realize significant cost savings.
- By integrating AI technology into its products, the company provides customers with compelling solutions and data-driven insights, strengthening its competitive edge in the industry.

Growth

- PlaxidityX has seen impressive 500% revenue growth since 2021, primarily fueled by its focus on automotive cybersecurity solutions. The substantial revenue increase has contributed to the company’s growth potential in securing the second position in the overall Growth index ranking.
- With over 100 granted and pending patents and an investment of over €150 million in the last 10 years, PlaxidityX demonstrates a commitment to developing innovative solutions tailored specifically to automotive cybersecurity.
- To date, PlaxidityX has secured more than 70 million vehicles across 45 production projects and 91 customers, indicating its strong revenue potential in the automotive cybersecurity industry.
- As of 2023, PlaxidityX has established offices in strategic locations, including Stuttgart, Detroit, South Korea, and Tokyo, reflecting its effort to expand its presence and growth potential across new regions.
- PlaxidityX not only caters to traditional passenger vehicles, but also extends its services to connected trucks, especially the 2W segment (which only has a handful of cybersecurity providers) and shared mobility fleet operators. This diversification within the automotive sector increases the company's total addressable market potential.

Frost Perspective

- PlaxidityX displays an exemplary array of partnerships with industry leaders to accelerate innovations and build a wide range of services and solutions, cementing its innovation leadership in the automotive cybersecurity space.
- Its vDome solution is a first-of-its-kind aftermarket anti-theft product that presents a viable opportunity to safeguard millions of connected vehicles on the road. This will likely be a significant growth engine for PlaxidityX in the next 3 to 5 years.
- The company stands out for its cybersecurity compliance services in the 2W segment, which includes motorcycles, scooters, and electric bicycles. PlaxidityX can differentiate itself further by developing dedicated security products for the niche 2W segment to establish a first-mover advantage and boost demand in the cybersecurity industry.
- With the automotive sector gearing up to transition toward electric and autonomous vehicles, there is a rising demand for securing data generated from these vehicles. PlaxidityX should contemplate exploring opportunities and addressing distinctive cybersecurity challenges for the smart mobility ecosystem, including V2X, V2G, and electric vehicle charging infrastructure communications.

Strategic Insights

1. Innovative monetization models are expected to capitalize on the future demand for cutting-edge security solutions. OEMs may transition toward usage-based pricing models, paying cybersecurity vendors based on the level of protection provided or the number of security incidents detected and prevented. Additionally, subscription-based services and pay-per-use arrangements could gain traction, offering OEMs flexibility and scalability in managing cybersecurity costs. By adapting their monetization strategies to evolving market dynamics, cybersecurity vendors can drive immense value for automotive stakeholders and foster long-term partnerships and revenue growth.

2. Collaboration among stakeholders in the automotive ecosystem will become necessary to effectively eliminate cyber threats. OEMs, suppliers, cybersecurity firms, regulatory bodies, and government agencies are expected to establish collaborative frameworks for sharing threat intelligence, best practices, and vulnerability disclosures. These ecosystems will foster a collective defense approach, enabling rapid identification and mitigation of emerging threats across the automotive supply chain.

3. As vehicles become software on wheels, the integration of generative AI technologies into cybersecurity solutions will be critical. Vendors should leverage generative AI to anticipate and adapt to evolving cyber threats in real time to strengthen the resilience of automotive cybersecurity systems. Moreover, the development of digital twins—virtual replicas of physical vehicles—will enable proactive threat detection and mitigation by simulating potential cyberattacks and vulnerabilities. This convergence of AI and cybersecurity will shape the future of automotive security strategies by emphasizing predictive and preemptive defense mechanisms.

4. In the coming years, governments across the globe will play a pivotal role in shaping the automotive cybersecurity landscape. With increased focus on road safety and safeguarding data privacy, regulatory bodies will introduce strict guidelines governing cybersecurity standards for connected and autonomous vehicles. This means automakers must adopt special initiatives to ensure compliance and invest substantially in cybersecurity measures to meet these regulations. These regulations will demand greater transparency and accountability in implementing cybersecurity practices. This will push OEMs to adopt aggressive risk assessment methodologies and uphold industry best practices to ensure the security of connected and autonomous vehicles.

Legal Disclaimer