2025 | Automotive & Smart Mobility Global Cybersecurity Report

Upstream

MIND THE CYBER GAP

2025 Predictions: The Future of Automotive Cybersecurity

As cyber threats grow in scale and complexity, industry leaders weigh in on the challenges and innovations that will define 2025. From AI-driven defenses to evolving regulations and expanding attack surfaces, these expert insights offer a glimpse into the road ahead for automotive cybersecurity.

Martin Arend

General Manager Automotive Security, BMW Group

As we look ahead to 2025, threats are expected to be on the rise within the Automotive ecosystem, increasingly driven by AI. These threats may target the vehicle itself, its backend systems, or the mobile applications that interact with it.

At BMW Group, maintaining a sharp focus on the effectiveness of our field measures is paramount to ensure we can respond swiftly and comprehensively. To meet these challenges, we will continue prioritizing the reliability and scalability of our detection systems, making them a cornerstone of our cybersecurity strategy.

Karin Shopen

VP of Product Management, Cisco Talos Intelligence Group, Cisco Security

Connected Autonomous Vehicles (CAVs) are a transformative innovation in transportation. However, like any new technology, they present associated cyber threats that could have financial consequences for organizations and physical safety risks for the public.

Due to increased vehicle connectivity, complex supply chains, and manufacturers' data monetization efforts, CAVs' attack surfaces are expansive—hence the importance and urgency of developing and executing a full-cycle security practice for CAVs and their ecosystem.

Wulf Schlachter

CEO, Management Advisory, DXBe

The risk of hacking EV charging infrastructure is a pressing concern, particularly as it intersects with critical IT systems and infrastructure. With charging networks becoming increasingly interconnected, they present new vulnerabilities for cybercriminals to exploit. A compromised charging station could act as a gateway for broader attacks, potentially jeopardizing other critical infrastructure such as the power grid or backend networks.

In the context of recent discussions around hybrid warfare, the growing digitization and interconnectedness of charging infrastructure heightens its appeal as a target for cyber threats. To mitigate these risks, EV charging operators and manufacturers must adopt robust cybersecurity standards and prioritize regular updates to safeguard against evolving threats.

Ozgur Tohumcu

General Manager, Automotive & Manufacturing, AWS

In 2025, the adoption of advanced SDV modules and ECU virtualization will deepen, driving the shift to end-to-end E/E architectures. Virtualized ECUs and tools will streamline vehicle software development, while Generative AI will accelerate workflows, enhance cybersecurity testing, and enable automated reasoning for assisted code remediation. OEMs will leverage Generative AI to strengthen security operations, detection, vulnerability management, and incident response capabilities.

The proliferation of AI will also push OEMs to adopt responsible AI practices and address the security challenges of automotive generative AI edge applications. Key considerations will include content moderation at the edge, securing OTA model updates, and safeguarding cyber-physical systems against foundation model theft via physical attacks. Despite significant investments in AI-driven cybersecurity, OEMs must continue prioritizing foundational security practices such as identity and access management, data protection, and threat modeling to ensure a robust defense against evolving threats.

Martin Hofmann

Chief Business Officer, Terra Quantum AG

The growing influence of global regulations such as UNECE WP.29 and the Cyber Resilience Act is pushing automakers to implement robust cybersecurity measures across their entire lifecycle and supply chain.

However, as the industry embraces electrification, AI, and autonomous technologies, cybersecurity has evolved from being merely a compliance necessity to a strategic competitive advantage.

These transformative technologies require a proactive and scalable approach to identifying and addressing cyber risks with far-reaching implications.

Vinod D'Souza

Office of the CISO, Head of Manufacturing and Industry, Google Cloud

In 2025, geopolitical tensions and state-sponsored cyberattacks will escalate risks for automotive manufacturers, targeting critical infrastructure and intellectual property. The convergence of IT and OT systems and reliance on interconnected technologies will expand the attack surface, exposing new vulnerabilities. Ransomware is also expected to grow more disruptive, focusing on production lines and supply chains, while AI-powered attacks will become more sophisticated, leveraging automation and ML to challenge defenses.

Continued adoption of AI by defenders will help them stay ahead of attackers in 2025, but a collaborative approach to cybersecurity is needed for effectively mitigating risks across the entire lifecycle and supply chain. Adopting secure cloud platforms and fostering greater information sharing will be key strategies for enhancing supply chain security and improving resilience in an interconnected ecosystem.

Tim Geiger

Senior Director, Vehicle and Connected Cyber Security, Ford Motor Company

Automakers face a growing cybersecurity challenge as connected vehicles become increasingly prevalent. APIs play a crucial role in enabling communication between vehicle systems, external devices, and cloud services. At the same time, attackers are becoming increasingly sophisticated in exploiting API vulnerabilities.

Safeguarding automotive APIs is essential to ensure the safety, privacy, and trust of connected vehicles as proactive measures today can prevent significant incidents tomorrow.

Mike Lexa

CISO & Vice President IT Infrastructure, CNH Industrial

In 2025, CISOs in the automotive industry will encounter heightened cybersecurity challenges driven by the proliferation of connected, autonomous, and electric vehicles. These innovations significantly expand the attack surface, introducing vulnerabilities in areas such as over-the-air updates, infotainment systems, and vehicle-to-everything (V2X) communications. Compounding these risks are stricter regulations, supply chain complexities, and the dual use of AI for both cyberattacks and defense.

To navigate this evolving landscape, CISOs must adopt robust cybersecurity frameworks, conduct rigorous vendor assessments, and implement proactive threat detection strategies. Prioritizing regulatory compliance, leveraging AI-driven cybersecurity solutions, and investing in workforce training will be essential to safeguarding against evolving threats.

Yoav Levy

CEO and Co-Founder, Upstream Security

As we look toward 2025, the cybersecurity landscape in the automotive industry is poised to become more complex than ever. Threat actors have already shifted toward large-scale, sophisticated attack methods, targeting not only vehicles but also interconnected systems such as EV charging infrastructure, API-driven companion apps, and dealership networks. This growing attack surface will demand a transformative and proactive approach to cybersecurity.

AI will take center stage in addressing these risks. While many OEMs have already made early investments, 2025 will see an acceleration in AI adoption, integrating it across detection, investigation, and mitigation processes. Real-time data processing will enable faster anomaly detection, more precise threat identification, and swift, automated responses—setting a new benchmark for protection in the mobility ecosystem. To navigate this evolving landscape, a forward-looking strategy combining advanced XDR and robust API security will be essential.