Cybersecurity For Cars - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

Cybersecurity For Cars Market Analysis

The Cybersecurity For Cars Market size is estimated at USD 4.09 billion in 2025, and is expected to reach USD 8.75 billion by 2030, at a CAGR of 16.40% during the forecast period (2025-2030). Rapid vehicle digitalization, growing regulatory scrutiny, and wider 5G/V2X roll-outs are reshaping competitive strategies and opening new service-led revenue pools. Manufacturers race to certify Cybersecurity Management Systems before UNECE R155/R156 audits, while cloud-native security platforms gain traction as software-defined vehicles demand continuous protection. Simultaneously, electric-vehicle adoption, bidirectional charging, and sensor-rich ADAS features multiply the attack surface, attracting specialized solution vendors that promise real-time threat intelligence and automated response. OEMs also eye monetization of over-the-air security updates and usage-based insurance programs that reward certified cyber-hardening, partially offsetting high integration costs.

Global Cybersecurity For Cars Market Trends and Insights

Regulatory mandates drive fundamental change

Global homologation now hinges on demonstrating end-to-end security. UNECE R155 alone creates a USD 2.1 billion compliance opportunity by 2030 as OEMs must track 69 attack vectors and prove continuous monitoring throughout vehicle lifecycles. ISO/SAE 21434 hardcodes cybersecurity engineering into concept and decommission phases, prompting carmakers to expand specialist teams. Similar rules emerge in Japan and the United States, eliminating first-mover disadvantages and standardizing

baselines worldwide.

Connected-vehicle fleet expansion multiplies attack surfaces

Modern cars host up to 150 ECUs and 100 million lines of code-volumes that could triple by 2030, stressing legacy defenses. Backend servers already account for 43% of incidents, and 95% of attacks originate remotely. 5G-based V2X exchanges add high-bandwidth vectors exposing telematics gateways, while ransomware targeting dealership IT highlights supply-chain vulnerabilities beyond the vehicle perimeter.

Legacy architecture integration costs constrain adoption

Retrofitting 150-plus ECUs in legacy platforms can add 15-20% to vehicle development budgets. Continental's 2022 breach illustrated supplier-network exposure and forced expensive architecture reviews. Such financial drag delays roll-outs among volume brands, even as compliance deadlines loom.

Other drivers and restraints analyzed in the detailed report include:

ADAS proliferation elevates safety-critical risks / Vehicle-to-Grid integration creates bidirectional pathways / Automotive cybersecurity talent shortage limits execution /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Software-based platforms held 41.2% of 2024 revenue, underscoring their centrality in a software-defined vehicle era where embedded firewalls, secure firmware, and runtime intrusion detection converge. Consulting-led offerings, however, are on a 19.8% CAGR ascent as OEMs outsource gap analyses, threat modeling, and audit preparation to specialist advisors. The cybersecurity for cars market increasingly rewards vendors capable of bundling continuous monitoring with UNECE R155 documentation support, a capability visible in HARMAN's end-to-end WP.29 packages.

Professional services also orchestrate multi-vendor integration when hardware security modules, PKI suites, and cloud SOC platforms must interoperate inside tight development timelines. Such cross-domain coordination positions service providers as primary gatekeepers of compliance roadmaps, shifting revenue toward recurring assessment and managed-detection contracts. Consequently, the cybersecurity for cars market is witnessing alliances where software licensors embed service retainer clauses to secure lifetime margins.

Endpoint controls retained a 30.1% share in 2024 because cryptographic keys, secure boot, and ECU-level firewalls remain foundational. Yet cloud defenses are racing ahead at 21.3% CAGR as automakers shift data lakes, OTA orchestration, and fleet analytics off-board. The cybersecurity for cars market size for cloud protection is swelling each quarter, buoyed by collaborations such as Upstream's tie-up with Google Cloud. Incident lessons from the 2024 Volkswagen data breach showed that insufficient encryption of telemetry can cascade into reputational damage.

Network-layer segmentation and TLS v1.3 upgrades ride parallel with cloud growth, while application-centric hardening becomes imperative as vehicles download microservices weekly. Wireless security remains the final mile, guarding 5G links that now underpin platooning and V2I signalling. As virtual ECUs offload tasks to the edge, hybrid architectures combining in-vehicle enforcement with remote AI-assisted analytics form the emerging blueprint across the cybersecurity for cars market.

Cybersecurity for Cars Market is Segmented by Solution Type (Software-Based, Hardware-Based, and More), Security Type (Network Security, Application Security, and More), Vehicle Type (Passenger Cars, Light Commercial Vehicles, and More), Application (Infotainment, Telematics and Connectivity, and More), Form Type (In-Vehicle and External Cloud Services), and Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

Asia-Pacific commanded 35.6% revenue in 2024 and is projected to grow at 20.2% CAGR, making it the fastest-advancing geography within the cybersecurity for cars market. China's scaling of connected-EV production fuels large-scale procurement of V2G-ready PKI and ECU hardening suites, while Japan's early alignment with UNECE rules accelerates supplier certification programs. South Korea's 5G highways amplify demand for real-time over-the-air patching technologies, and India's emergent export ambitions trigger investments in ISO 21434 compliance tooling. Collectively, these dynamics push regional vendors to deliver low-latency cloud SOC services hosted within data-residency-compliant zones.

North America represents a mature yet evolving arena where premium vehicle trims and robust insurance ecosystems encourage cybersecurity monetization. The United States Connected Vehicles Rule, effective March 2025, forces OEMs to audit supply chains for sanctioned components, redirecting procurement toward domestic chipsets and security modules. Canada's tier-one suppliers leverage proximity and regulatory alignment to integrate secure Ethernet backbones, while Mexico's assembly plants adopt managed-security services to counter rising ransomware aimed at just-in-time logistics.

Europe remains a regulatory trendsetter and R&D hub. Germany hosts flagship suppliers such as Bosch ETAS and Continental, although the latter's prior breach highlighted vulnerabilities in centralized architecture. France and the United Kingdom channel public grants into quantum-safe automotive cryptography, while the ENX VCS audit framework overlays ISO 21434 to standardize supplier assessments. Eastern European engineering hubs contribute competitive talent, though war-related cyber sanctions reshape sourcing strategies.

List of Companies Covered in this Report:

Continental AG / Harman International (Samsung) / Bosch ETAS GmbH / Infineon Technologies AG / NXP Semiconductors NV / Cisco Systems Inc. / DENSO Corporation / Visteon Corporation / Delphi Technologies plc / Honeywell International Inc. / Argus Cyber Security Ltd. / Karamba Security Ltd. / Arilou Technologies Ltd. / Escrypt GmbH / Secunet Security Networks AG / Upstream Security Ltd. / VicOne Inc. (Trend Micro) / GuardKnox Cyber-Technologies Ltd. / BlackBerry QNX / SafeRide Technologies Ltd. / Cybellum Technologies Ltd. / Trillium Secure Inc. / Vector Informatik GmbH / Comsec Automotive Ltd. / GuardSquare NV / AutoCrypt Co. Ltd. /

Additional Benefits:

The market estimate (ME) sheet in Excel format /
3 months of analyst support /

Table of Contents:

Cybersecurity For Cars - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-27
		Signature