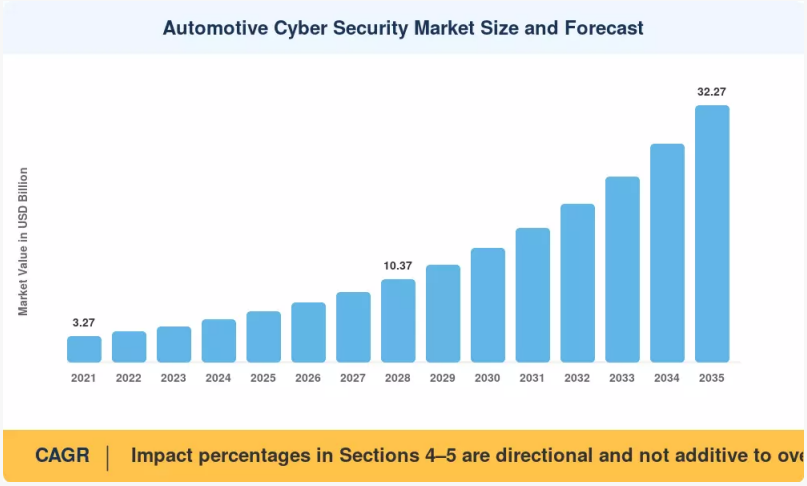
Automotive Cybersecurity Market Share Projected To Reach USD 32.27 Billion, at a 17.6% CAGR Across the Forecast 2035

Embedded Security Software accounted for a 40.5% share of the Automotive Cybersecurity Market in 2024, driven by OEM demand for tamper-proof firmware layers.



Automotive Cybersecurity Market Summary

NY, CA, UNITED STATES, July 14, 2026 /EINPresswire.com/ -- Automotive cybersecurity encompasses the comprehensive set of practices, technologies, and strategies designed to protect vehicles and their connected systems from cyber threats, unauthorized access, and malicious attacks . As modern vehicles evolve into sophisticated connected devices, cybersecurity has become essential for securing critical vehicle components including infotainment systems, telematics, autonomous driving technologies, and vehicle-to-everything (V2X) communications . The discipline includes encryption, intrusion detection systems (IDS), firewalls, secure over-the-air (OTA) updates, and threat monitoring, ensuring the confidentiality, integrity, and availability of vehicle systems and data . With the increasing connectivity of vehicles, robust cybersecurity is essential to protect both the vehicle and its occupants from potential cyber risks.

> Vehicle/On-board Systems Security held a 49.2% revenue share of the Automotive Cybersecurity Market in 2024, reflecting concentrated spend on in-vehicle intrusion prevention.”
>
> *Arti Dhapte*

Automotive Cybersecurity Market Overview

The automotive cybersecurity market share is positioned for extraordinary growth through 2035, driven by the accelerating transition to connected, autonomous, and software-defined vehicles, the rising incidence of sophisticated cyberattacks, and the implementation of stringent regulatory mandates. The projected valuation of USD 32.27 billion, growing at a robust CAGR of 17.6%, reflects the

evolution of cybersecurity from a niche specialty to an essential automotive safety discipline.

The market is experiencing explosive growth driven by several fundamental factors. The rapid evolution toward connected, autonomous, and software-defined vehicles is a primary growth driver, as modern vehicles increasingly rely on IoT, cloud integration, and OTA updates, expanding the attack surface for cyber threats . High-profile incidents, such as the 2015 hacking of a Jeep Cherokee where researchers remotely accessed steering and braking functions, demonstrated the vulnerabilities of connected vehicles and raised industry-wide alarms . The rise of sophisticated cyberattacks—with global cyber incidents in the automotive sector reaching an all-time high and 92% of attacks carried out remotely—is driving substantial investment in advanced security technologies . Stringent regulatory mandates, including UN Regulation No. 155 for the EU and ISO/SAE 21434 standards, compel manufacturers to implement comprehensive cybersecurity measures throughout the vehicle lifecycle .

Industry trends indicate a decisive shift from reactive security measures toward predictive and collaborative defense approaches. Manufacturers are moving from one-off defenses to ecosystem-wide protection, leveraging AI, cloud analytics, and threat intelligence networks . Vehicle Security Operations Centers (VSOCs) providing 24/7 real-time fleet protection, AI-driven adaptive firewalls that evolve automatically with new threat patterns, and collaborative cyber networks enabling shared intelligence between OEMs, suppliers, and governments are emerging as key trends . The integration of security-by-design principles throughout the vehicle development lifecycle—from concept through production—is becoming standard practice as security retrofits are less reliable and more costly .

The demand outlook remains exceptionally strong. North America remains the largest market, driven by advanced EV infrastructure and leading cybersecurity firms . Europe is the fastest-growing region for compliance-driven innovation, anchored by UN R155 and the EU Cyber Resilience Act . Asia-Pacific is emerging as the growth engine, fueled by surging connected car production and EV adoption across China, Japan, South Korea, and India . The software segment is expected to dominate the market, driven by the increasing importance of secure development lifecycle practices and OTA capabilities . As the industry continues to integrate advanced technologies like V2X and autonomous driving, market growth is expected to accelerate, making automotive cybersecurity a critical safety discipline essential for consumer trust and regulatory compliance.

 Get Free Sample Report for Detailed Market Insights:

https://www.marketresearchfuture.com/sample_request/2970

Automotive Cybersecurity Market Segmentation

By Security Domain

The automotive cybersecurity market is segmented by security domain into Vehicle/On-board Systems Security, Backend & Telecom Security, and Production (OT and IIoT) Security. Vehicle/on-board systems security encompasses protection for ECUs, infotainment, telematics, ADAS, and V2X communication modules . This segment is critical for protecting in-vehicle networks, including the CAN bus, from intrusion and manipulation. Backend and telecom security focuses on protecting cloud platforms, telematics servers, and communication channels that connect vehicles to external networks, including 5G and V2X infrastructure . Production security addresses operational technology (OT) and industrial IoT (IIoT) security in manufacturing environments, protecting against threats to production systems and ensuring secure software supply chains .

By Solution Type

Solution segmentation includes Embedded Security Software, Hardware Security Modules, Cloud-based Security Platforms, and Professional Services. Embedded security software encompasses runtime protection on ECUs, secure boot, and application security layers integrated into vehicle systems . Hardware security modules provide hardware-based root of trust, secure key storage, and cryptographic functions essential for secure communication and authentication . Cloud-based security platforms offer fleet threat detection, analytics, and centralized monitoring services, complementing in-vehicle security . Professional services include vulnerability assessment, secure development lifecycle consulting, incident response, and post-market telemetry services, which are fast-growing service lines . The software segment is expected to dominate the market by 2030 .

By Deployment Model

Deployment model segmentation includes On-Premises, Cloud, and Hybrid solutions. On-premises solutions are typically deployed within OEM or supplier environments for in-vehicle security and internal systems management. Cloud-based platforms provide fleet-wide security monitoring, threat intelligence, and over-the-air update management services, enabling centralized threat detection and real-time telemetry . Hybrid deployments combine both approaches, using local prevention on ECUs with centralized cloud monitoring to create a comprehensive security architecture .

By End User

End-user segmentation covers OEMs, Tier-1 Suppliers, Smart-Factory Operators, and Aftermarket & Fleet Operators. OEMs represent the largest segment, as they are responsible for integrating cybersecurity into new vehicle platforms and ensuring compliance with regulatory mandates throughout the vehicle lifecycle . Tier-1 suppliers provide components and subsystems with embedded security features, increasingly required by OEMs to meet ISO/SAE 21434 compliance . Smart-factory operators address OT and IIoT security in manufacturing

environments, protecting production systems from cyber threats. Aftermarket and fleet operators represent a growing segment as connected fleets require comprehensive security management and monitoring solutions .

By Region

Regional segmentation includes North America, Europe, Asia-Pacific, South America, and the Middle East and Africa. North America holds the highest share of the global market, supported by strong government support and advanced EV infrastructure . Europe is the fastest-growing region for regulatory-driven adoption, with Germany and the UK leading compliance efforts . Asia-Pacific is emerging as the growth engine, driven by connected car production surges in China, Japan, South Korea, and India .

 You can buy this market report at:

https://www.marketresearchfuture.com/checkout?currency=one_user-USD&report_id=2970

Automotive Cybersecurity Market Competitive Landscape

The automotive cybersecurity market exhibits moderate concentration, with a broad ecosystem of competitors and collaborators including tier-1 suppliers, specialized cybersecurity vendors, semiconductor and OS vendors, cloud providers, and consultancies . The top three players occupy about 25% of the global market . Partnerships and M&A are common as OEMs seek turnkey security stacks and regulatory compliance . Key companies include Continental AG (Aumovio SE), Robert Bosch GmbH, Denso Corporation, Harman International, NXP Semiconductors, Aptiv, Infineon Technologies, Renesas Electronics, BlackBerry Limited, Argus Cyber Security, Karamba Security, GuardKnox, Upstream Security, ETAS, Cybellum, and VicOne Inc. .

Continental AG is a leading Tier-1 supplier offering comprehensive cybersecurity solutions, including Aumovio SE for automotive cybersecurity services and secure gateways . Robert Bosch GmbH provides embedded security software, ECU hardening, and secure OTA solutions integrated into its broad automotive electronics portfolio . Denso Corporation serves as a Toyota ecosystem anchor supplier, offering CAN-bus security modules and keyless entry systems . Harman International focuses on connected-vehicle security platforms and OTA update management, leveraging Samsung's ecosystem integration . NXP Semiconductors provides hardware security modules, secure elements, and microcontroller-based solutions for automotive applications .

Strategic developments include partnerships and collaborations to strengthen technology integration—HL Mando Corporation partnered with Argus Cyber Security in 2023 to integrate its CAN Intrusion Detection System into the company's electrification systems . Differentiation

increasingly hinges on embedded vs. cloud-centric approaches, with the most effective solutions blending local prevention and centralized monitoring . Vendors also differentiate through lifecycle services and alignment with ISO/SAE 21434 standards, secure boot, and hardware root-of-trust implementations .

Latest Industry News & Developments

Recent industry developments highlight the accelerating transformation of the automotive cybersecurity market. In 2023, HL Mando Corporation partnered with Argus Cyber Security to integrate its CAN Intrusion Detection System into the company's electrification systems, such as brakes and steering, showcasing the industry's focus on enhancing cyber resilience . The partnership highlights the trend toward integrating real-time IDS with V2X communication technologies to detect and neutralize cyber threats continuously .

The European Union's UN Regulation No. 155 became effective in July 2022, mandating that all new vehicles sold in the EU must be equipped with robust cybersecurity measures, including secure software development, vulnerability detection, and incident response protocols . This regulation ensures manufacturers prioritize cybersecurity throughout the vehicle lifecycle, from design to production . The UN's Regulation No. 156 further addresses over-the-air software updates, ensuring vehicles remain secure throughout their lifecycle .

The US Department of Transportation's evolving AV 4.0 policy framework and NHTSA's push for higher cybersecurity standards are shaping the US market . The market is also witnessing the emergence of Vehicle Security Operations Centers (VSOCs) providing 24/7 real-time fleet protection, AI-driven adaptive firewalls, and collaborative cyber networks enabling shared intelligence between OEMs, suppliers, and governments . The shift toward predictive and collaborative defense approaches characterizes the next era of automotive cybersecurity, with manufacturers moving from one-off defenses to ecosystem-wide protection .

Automotive Cybersecurity Market Challenges & Opportunities

Key restraints facing the automotive cybersecurity market include the high complexity and cost of implementing comprehensive cybersecurity solutions across vehicle architectures, which creates barriers for smaller manufacturers and suppliers . The shortage of skilled cybersecurity professionals with automotive domain expertise creates talent acquisition challenges . Evolving cyber threats require continuous innovation, as attackers become increasingly sophisticated . Complex supply chains with multiple vendors creating security blind spots , high integration costs, and consumer resistance to subscription-based security models further constrain growth. The challenge of securing legacy vehicles with limited update paths remains a significant issue .

Emerging opportunities are substantial and diverse. The increasing regulatory requirements, including UN R155 and ISO/SAE 21434, create significant market opportunities for companies providing advanced cybersecurity solutions . The increasing development of autonomous

vehicles creates demand for specialized cybersecurity solutions to protect AI-based systems and V2X communication . The adoption of AI and machine learning for predictive threat detection enables proactive security measures . The expansion of V2X technology requires secure communication channels and hardware security modules . Growth of managed security services and cloud-based solutions offers recurring revenue opportunities . The rise of software-defined vehicles creates opportunities for secure OTA update platforms and software lifecycle management services .

Future potential lies in the development of predictive, AI-powered threat detection systems, the integration of quantum-resistant cryptography, and the adoption of zero-trust architectures for vehicle networks . The establishment of Vehicle SOCs providing real-time fleet protection and the growth of collaborative cyber networks enabling shared threat intelligence will reshape the market . Companies that successfully innovate in AI-driven security, build strategic partnerships with OEMs, and develop integrated hardware-software security stacks will capture disproportionate value. As automotive and IT ecosystems continue to converge, cybersecurity must become a core design principle, not a retrofit solution .

To explore more market insights, visit us at:

https://www.marketresearchfuture.com/reports/automotive-cyber-security-market-2970

The medium-term growth outlook remains exceptionally strong, supported by UN R155 compliance requirements, the expansion of V2X communication, and the increasing adoption of AI-driven security solutions. North America will continue to lead in revenue terms, while Europe will experience the fastest regulatory-driven growth and Asia-Pacific will emerge as the growth engine due to surging connected car production.

Long-term industry potential extends well beyond the current forecast horizon, as the convergence of autonomous driving, AI, and connectivity creates new security requirements and revenue models. The adoption of predictive, AI-powered threat detection, the integration of zero-trust architectures, and the emergence of Vehicle Security Operations Centers will reshape the market landscape. Companies that successfully innovate in embedded security software, hardware security modules, and cloud-based fleet monitoring, while building strategic partnerships across the automotive ecosystem, will capture disproportionate value. As the cars of tomorrow depend as much on secure software and architectures as they do on mechanical engineering today , automotive cybersecurity will remain essential to ensuring consumer trust, vehicle safety, and the future of connected mobility.

More Related Reports from MRFR Library:

https://www.marketresearchfuture.com/reports/automotive-electric-power-steering-market-5743

https://www.marketresearchfuture.com/reports/automotive-radar-sensors-market-5860

https://www.marketresearchfuture.com/reports/automotive-secondary-wiring-harness-market-6091

https://www.marketresearchfuture.com/reports/autonomous-trucks-market-6126

https://www.marketresearchfuture.com/reports/electric-truck-market-6261

https://www.marketresearchfuture.com/reports/electric-power-steering-system-market-6263

https://www.marketresearchfuture.com/reports/automotive-fuel-rail-market-6272

https://www.marketresearchfuture.com/reports/automotive-steer-by-wire-system-market-6389

https://www.marketresearchfuture.com/reports/cng-vehicles-market-6497

https://www.marketresearchfuture.com/reports/automotive-differential-system-market-7124

Larry Wilson
WantStats Research And Media Pvt. Ltd.
+1 855-661-4441
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X
