

Automotive Cybersecurity Market Opportunity, Growth Drivers, Industry Trend Analysis, and Forecast 2025 - 2034

<https://marketpublishers.com/r/ACBA2611FEB9EN.html>

Date: August 2025

Pages: 345

Price: US\$ 4,850.00 (Single User License)

ID: ACBA2611FEB9EN

Abstracts

The Global Automotive Cybersecurity Market was estimated at USD 3.52 billion in 2024. The market is expected to grow from USD 3.87 billion in 2025 to USD 10.42 billion by 2034 at a CAGR of 11.6%, according to latest report published by Global Market Insights Inc.

As vehicles become increasingly connected via V2X (vehicle-to-everything) communications and embedded infotainment systems, the attack surface for hackers grows significantly. This pushes automakers to invest in robust cybersecurity solutions to protect real-time data exchange, vehicle networks, and digital systems.

Rising demand in Passenger Vehicle

The passenger vehicle segment in the automotive cybersecurity market held sustainable share in 2024, owing to the rapid growth of connected cars, infotainment systems, and autonomous driving technologies. As consumers expect smarter, safer, and more digital driving experiences, automakers are integrating advanced cybersecurity protocols directly into passenger vehicles.

Growing Adoption of In-Vehicle Cybersecurity

In-vehicle cybersecurity segment held substantial share in 2024 driven by the focus on safeguarding electronic control units (ECUs), infotainment systems, telematics, and vehicle networks from external threats. As vehicles increasingly function like mobile computers, in-vehicle cybersecurity ensures real-time threat detection, secure communication, and data integrity. OEMs are now designing security from the ground

up, embedding software firewalls, intrusion detection systems, and encryption directly into vehicle hardware and software stacks.

Application to Gain Traction

The application segment in automotive cybersecurity market generated notable revenues in 2024 fueled by telematics and infotainment to ADAS (Advanced Driver Assistance Systems) and powertrain control. Every digital touchpoint inside a modern vehicle needs protection. As the complexity of vehicle architecture grows, cybersecurity applications are being tailored to each system, ensuring end-to-end protection.

North America to Emerge as a Lucrative Region

North America automotive cybersecurity market held robust growth in 2024 driven by strong regulatory backing, tech-savvy consumers, and the presence of leading cybersecurity and automotive innovators. The U.S. sets embedding cyber resilience in mobility solutions. With regulatory frameworks like the U.S. Cybersecurity Executive Order and rising consumer awareness around data privacy, automakers are accelerating investments in robust in-vehicle security systems. Additionally, partnerships between OEMs and major tech firms are fueling new breakthroughs in vehicle security protocols.

Major players in the automotive cybersecurity market are Karamba Security, Lear, Harman International, Denso, Upstream Security, NXP, Blackberry, Aptiv, Continental, Intertek.

Companies in the automotive cybersecurity market are focusing on innovation through extensive R&D to develop cutting-edge security solutions that address emerging threats in connected and autonomous vehicles. Strategic partnerships and collaborations with automakers, technology providers, and regulatory bodies are accelerating product integration and compliance. Many players are investing heavily in real-time threat detection systems and AI-driven cybersecurity frameworks to enhance vehicle safety. Expanding their global footprint through acquisitions and joint ventures is another common tactic to capture new markets and customer segments.

Contents

CHAPTER 1 METHODOLOGY

- 1.1 Research design
 - 1.1.1 Research approach
 - 1.1.2 Data collection methods
 - 1.1.3 GMI proprietary AI system
 - 1.1.3.1 AI-Powered research enhancement
 - 1.1.3.2 Source consistency protocol
 - 1.1.3.3 AI accuracy metrics
- 1.2 Base estimates and calculations
 - 1.2.1 Base year calculation
- 1.3 Forecast model
 - 1.3.1 Key trends for market estimates
 - 1.3.2 Quantified market impact analysis
 - 1.3.2.1 Mathematical impact of growth parameters on forecast
 - 1.3.3 Scenario Analysis Framework
- 1.4 Primary research & validation
- 1.5 Some of the primary sources (but not limited to)
- 1.6 Data mining sources
 - 1.6.1 Secondary
 - 1.6.1.1 Paid Sources
 - 1.6.1.2 Public Sources
 - 1.6.1.3 Sources, by region
- 1.7 Research Trail & Confidence Scoring
 - 1.7.1 Research Trail Components:
 - 1.7.2 Scoring Components
- 1.8 Research transparency addendum
 - 1.8.1 Source attribution framework
 - 1.8.2 Quality assurance metrics
 - 1.8.3 Our commitment to trust

CHAPTER 2 EXECUTIVE SUMMARY

- 2.1 Industry 360° synopsis, 2021 - 2034
- 2.2 Key market trends
 - 2.2.1 Regional
 - 2.2.2 Vehicle

- 2.2.3 Security
- 2.2.4 Form
- 2.2.5 Application
- 2.2.6 Deployment Mode
- 2.3 TAM Analysis, 2025-2034
- 2.4 CXO perspectives: Strategic imperatives
 - 2.4.1 Executive decision points
 - 2.4.2 Critical success factors
- 2.5 Future outlook and strategic recommendations

CHAPTER 3 INDUSTRY INSIGHTS

- 3.1 Industry ecosystem analysis
 - 3.1.1 Supplier landscape
 - 3.1.1.1 Automotive OEM
 - 3.1.1.2 Cybersecurity solution providers
 - 3.1.1.3 Cloud service providers
 - 3.1.1.4 Tier 1 Suppliers
 - 3.1.1.5 Technology integrators
 - 3.1.1.6 End users
 - 3.1.2 Profit margin analysis
 - 3.1.3 Cost structure
 - 3.1.4 Value addition at each stage
 - 3.1.5 Factor affecting the value chain
 - 3.1.6 Disruptions
- 3.2 Industry impact forces
 - 3.2.1 Growth drivers
 - 3.2.1.1 Growing connected vehicle adoption
 - 3.2.1.2 Strict cybersecurity regulations for automotive manufacturers
 - 3.2.1.3 Growing complexity of vehicle architecture
 - 3.2.1.4 Proliferation of Over-the-Air Updates
 - 3.2.2 Industry pitfalls and challenges
 - 3.2.2.1 Cost constraints in the implementation of cybersecurity solutions
 - 3.2.2.2 Legacy system integration
 - 3.2.3 Market opportunities
 - 3.2.3.1 Rising connected vehicle adoption
 - 3.2.3.2 Shift toward software-defined vehicles
 - 3.2.3.3 Regulatory push and compliance standards
 - 3.2.3.4 Expansion of EVs and autonomous vehicles

3.3 Regulatory landscape

3.3.1 North America

3.3.2 Europe

3.3.3 Asia Pacific

3.3.4 Latin America

3.3.5 Middle East & Africa

3.4 Porter's analysis

3.5 PESTEL analysis

3.6 Technology and Innovation landscape

3.6.1 Current technological trends

3.6.1.1 Traditional security approaches and limitations

3.6.1.2 Next-generation security architecture

3.6.1.3 Integration with automotive development processes

3.6.2 Emerging technologies

3.6.2.1 Artificial intelligence and machine learning applications

3.6.2.2 Behavioral analytics and anomaly detection

3.6.2.3 Blockchain for secure vehicle communications

3.6.2.4 Quantum computing impact on cryptography

3.6.3 Zero trust security architecture

3.6.3.1 Implementation of strategies for automotive systems

3.6.3.2 Network segmentation and micro-segmentation

3.6.3.3 Identity and access management (IAM) solutions

3.6.4 Software-defined vehicle (SDV) security

3.6.4.1 Security-by-design principles

3.6.4.2 Continuous security monitoring

3.6.4.3 Dynamic security policy management

3.6.5 Future technology disruptions (2025-2034)

3.6.5.1 Quantum-resistant cryptography implementation

3.6.5.2 6G network security requirements

3.6.5.3 Edge computing security challenges

3.6.5.4 Autonomous vehicle security evolution

3.6.6 Technology Readiness Level (TRL) Assessment

3.6.6.1 Current technology maturity analysis

3.6.6.2 Commercialization timeline projections

3.6.6.3 Investment requirements and ROI analysis

3.7 Patent analysis

3.8 Pricing trends and economic analysis

3.9 Cost Analysis and ROI Assessment

3.9.1 Cybersecurity investment analysis

- 3.9.2 CSMS implementation cost assessment
- 3.9.3 Incident cost impact analysis
- 3.9.4 Regional cost variations
- 3.9.5 Cost optimization strategies
- 3.9.6 Financial risk assessment
- 3.10 Threat intelligence and attack analysis
 - 3.10.1 Current threat landscape assessment
 - 3.10.2 Attack vector classification and analysis
 - 3.10.3 Critical system vulnerabilities
 - 3.10.4 Advanced persistent threat (APT) analysis
 - 3.10.5 Incident response and forensics capabilities
 - 3.10.6 Threat intelligence sharing and collaboration
- 3.11 Use cases
- 3.12 Investment landscape and funding analysis
- 3.13 Cost-benefit analysis
- 3.14 Best-case scenario

CHAPTER 4 COMPETITIVE LANDSCAPE, 2024

- 4.1 Introduction
- 4.2 Company market share analysis
 - 4.2.1 North America
 - 4.2.2 Europe
 - 4.2.3 Asia Pacific
 - 4.2.4 LATAM
 - 4.2.5 MEA
- 4.3 Competitive analysis of major market players
- 4.4 Competitive positioning matrix
- 4.5 Strategic outlook matrix
- 4.6 Key developments
 - 4.6.1 Mergers & acquisitions
 - 4.6.2 Partnerships & collaborations
 - 4.6.3 New Product Launches
 - 4.6.4 Expansion Plans and funding

CHAPTER 5 MARKET ESTIMATES & FORECAST, BY VEHICLE, 2021 - 2034 (\$BN)

- 5.1 Key trends
- 5.2 Passenger vehicles

5.2.1 Hatchback

5.2.2 Sedan

5.2.3 SUV

5.3 Commercial vehicle

5.3.1 Light commercial vehicle (LCVs)

5.3.2 Medium commercial vehicle (MCVs)

5.3.3 Heavy commercial vehicle (HCVs)

CHAPTER 6 MARKET ESTIMATES & FORECAST, BY SECURITY, 2021 - 2034 (\$BN)

6.1 Key trends

6.2 Application

6.3 Network

6.4 Endpoint

CHAPTER 7 MARKET ESTIMATES & FORECAST, BY DEPLOYMENT MODE, 2021 - 2034 (\$BN)

7.1 Key trends

7.2 Cloud-based

7.3 On-premises

7.4 Hybrid

CHAPTER 8 MARKET ESTIMATES & FORECAST, BY APPLICATION, 2021 - 2034 (\$BN)

8.1 Key trends

8.2 ADAS & safety

8.3 Body control & comfort

8.4 Infotainment

8.5 Telematics

8.6 Powertrain systems

8.7 Communication systems

CHAPTER 9 MARKET ESTIMATES & FORECAST, BY FORM, 2021 - 2034 (\$BN)

9.1 Key trends

9.2 In-vehicle cybersecurity

9.3 External cloud cybersecurity

CHAPTER 10 MARKET ESTIMATES & FORECAST, BY REGION, 2021 - 2034 (\$BN)

10.1 Key trends

10.2 North America

10.2.1 US

10.2.2 Canada

10.3 Europe

10.3.1 Germany

10.3.2 UK

10.3.3 France

10.3.4 Italy

10.3.5 Spain

10.3.6 Russia

10.3.7 Nordics

10.4 Asia Pacific

10.4.1 China

10.4.2 India

10.4.3 Japan

10.4.4 Australia

10.4.5 South Korea

10.4.6 Philippines

10.4.7 Indonesia

10.5 Latin America

10.5.1 Brazil

10.5.2 Mexico

10.5.3 Argentina

10.6 MEA

10.6.1 South Africa

10.6.2 Saudi Arabia

10.6.3 UAE

CHAPTER 11 COMPANY PROFILES

11.1 Global Players

11.1.1 Argus Cyber Security

11.1.2 Blackberry

11.1.3 Bosch

- 11.1.4 BT Group
- 11.1.5 Cisco Systems
- 11.1.6 Continental
- 11.1.7 Denso
- 11.1.8 ESCRYPT
- 11.1.9 Harman International
- 11.1.10 Intel
- 11.1.11 Irdeto Automotive
- 11.1.12 Karamba Security
- 11.1.13 Lear Corporation
- 11.1.14 Microsoft
- 11.1.15 NXP Semiconductors
- 11.1.16 Symantec
- 11.1.17 Trillium Secure
- 11.1.18 Vector Informatik
- 11.2 Regional Players
 - 11.2.1 Aptiv
 - 11.2.2 Eneos Cyber Solutions
 - 11.2.3 Intertek
 - 11.2.4 OneLayer
 - 11.2.5 SafeRide Technologies
 - 11.2.6 Tuxera Automotive
- 11.3 Emerging Players
 - 11.3.1 Arilou Technologies
 - 11.3.2 AutoCrypt
 - 11.3.3 GuardKnox
 - 11.3.4 Karamba Security
 - 11.3.5 Keen Security Lab
 - 11.3.6 Upstream Security

I would like to order

Product name: Automotive Cybersecurity Market Opportunity, Growth Drivers, Industry Trend Analysis, and Forecast 2025 - 2034

Product link: <https://marketpublishers.com/r/ACBA2611FEB9EN.html>

Price: US\$ 4,850.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/ACBA2611FEB9EN.html>