

Vehicle-to-everything (V2X) Security Chips Market Opportunity, Growth Drivers, Industry Trend Analysis, and Forecast 2025 - 2034

<https://marketpublishers.com/r/V1EF420D2F09EN.html>

Date: October 2025

Pages: 209

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

ID: V1EF420D2F09EN

Abstracts

The Global Vehicle-to-everything Security Chips Market was valued at USD 681.8 million in 2024 and is estimated to grow at a CAGR of 19.1% to reach USD 3.9 billion by 2034.

Rising adoption of automated driving, connected vehicles, and advanced driver-assistance features is rapidly transforming the landscape for in-vehicle security hardware. Automakers are increasingly embedding components such as AI accelerators, radar interfaces, signal processors, and secure microcontrollers to improve situational awareness, decision-making, and system resilience. A growing emphasis on regulatory compliance, cyber protection, and real-time responsiveness has pushed manufacturers to design chips with embedded encryption and automotive-grade certifications. The pandemic spotlighted the fragility of global chip supply chains, which accelerated the push for regional manufacturing, end-to-end validation, and scalable security architectures. As electric mobility and autonomous fleets expand, demand for secure vehicle communication systems continues to climb. Subscription-based encryption updates, integrated software-hardware co-design, and Security-as-a-Service (SECaaS) offerings are being used to provide ongoing protection across evolving threat landscapes.

The vehicle-to-vehicle (V2V) communication systems segment accounted for a 37% share in 2024 and is expected to grow at a CAGR of 19% through 2034. This growth is driven by the increasing need for safe and responsive data exchanges between vehicles. Security chips within V2V architectures are critical for shielding traffic data, collision alerts, and system commands from cyber threats, ensuring safe and authenticated communication across vehicles in motion.

In 2024, the original equipment manufacturers (OEMs) segment held a 73% share and is projected to grow at a CAGR of 18.1% by 2034. The high share is linked to the direct integration of secure connectivity features into vehicle platforms at the production stage. Compliance with standards like ISO/SAE 21434 and UNECE WP.29 is now a priority, prompting automakers to hardwire V2X security into their systems to counter threats such as spoofing and unauthorized access, while enhancing user trust and brand integrity.

US Vehicle-to-everything (V2X) Security Chips Market held an 86% share in 2024, generating USD 197.3 million. Market momentum in the US is largely supported by federal safety regulations, the expansion of intelligent transport systems, and rapid growth in autonomous mobility. Federal bodies are reinforcing the need for V2X protocols, encouraging automakers and component suppliers to implement tamper-proof microcontrollers, hardware encryption engines, and root-of-trust frameworks to secure data flow and maintain compliance across connected vehicle platforms.

Key companies in the Global Vehicle-to-everything (V2X) Security Chips Market are Denso, Qualcomm Technologies, NXP Semiconductors, Renesas Electronics, Bosch, Infineon Technologies, ST Microelectronics, Huawei Technologies, Autotalks, and Continental. Leading firms in the Vehicle-to-everything (V2X) Security Chips Market are focusing on developing dedicated hardware security modules, secure boot protocols, and over-the-air (OTA) cryptographic key management systems to safeguard communication channels in connected vehicles. These players are actively co-developing solutions with OEMs and Tier-1 suppliers to ensure chips meet functional safety and data protection standards. Several companies are investing in AI-powered security engines capable of real-time threat detection at the edge.

Contents

CHAPTER 1 METHODOLOGY

- 1.1 Market scope and definition
- 1.2 Research design
 - 1.2.1 Research approach
 - 1.2.2 Data collection methods
- 1.3 Data mining sources
 - 1.3.1 Global
 - 1.3.2 Regional/Country
- 1.4 Base estimates and calculations
 - 1.4.1 Base year calculation
 - 1.4.2 Key trends for market estimation
- 1.5 Primary research and validation
 - 1.5.1 Primary sources
- 1.6 Forecast model
- 1.7 Research assumptions and limitations

CHAPTER 2 EXECUTIVE SUMMARY

- 2.1 Industry 360° synopsis, 2021 - 2034
- 2.2 Key market trends
 - 2.2.1 Regional
 - 2.2.2 Vehicle Autonomy Integration
 - 2.2.3 Security Chip
 - 2.2.4 Component
 - 2.2.5 Vehicle
 - 2.2.6 Application
 - 2.2.7 End Use
- 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
- 3.1.2 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 Rising need for data protection in connected vehicles.
 - 3.2.1.2 Government cybersecurity mandates accelerating growth.
 - 3.2.1.3 5G and edge computing enable faster, secure V2X communication.
 - 3.2.1.4 Smart city initiatives boost secure vehicle communication adoption.
 - 3.2.2 Industry pitfalls & challenges
 - 3.2.2.1 High costs associated with implementing V2X security chips are limiting adoption among manufacturers
 - 3.2.2.2 Lack of standardized security protocols across vehicles and infrastructure is creating deployment challenges.
 - 3.2.3 Market opportunities
 - 3.2.3.1 Autonomous vehicle adoption increases demand for advanced security.
 - 3.2.3.2 Electric vehicle growth drives secure charging and communication needs.
 - 3.2.3.3 5G-enabled vehicles open new chip design opportunities.
 - 3.2.3.4 V2X integration with smart infrastructure enables new services.
- 3.3 Growth potential analysis
- 3.4 Regulatory landscape
 - 3.4.1 North America
 - 3.4.2 Europe
 - 3.4.3 Asia Pacific
 - 3.4.4 Latin America
 - 3.4.5 Middle East & Africa
- 3.5 Porter's analysis
- 3.6 PESTEL analysis
- 3.7 Technology and Innovation landscape
 - 3.7.1 Current technological trends
 - 3.7.2 Emerging technologies
- 3.8 Price trends
 - 3.8.1 By region
 - 3.8.2 By Products
- 3.9 Production statistics
 - 3.9.1 Production hubs

- 3.9.2 Consumption hubs
- 3.9.3 Export and import
- 3.10 Cost breakdown analysis
- 3.11 Patent analysis
- 3.12 Sustainability and environmental aspects
 - 3.12.1 Sustainable practices
 - 3.12.2 Waste reduction strategies
 - 3.12.3 Energy efficiency in production
 - 3.12.4 Eco-friendly initiatives
 - 3.12.5 Carbon footprint considerations
- 3.13 Future Outlook & Technology Roadmap
 - 3.13.1. Next-Generation V2 X Security Technologies
 - 3.13.2. Quantum-Safe V2 X Communication
 - 3.13.3 AI-Driven Security Threat Detection
 - 3.13.4. Zero-Trust V2 X Architecture
 - 3.13.5. Blockchain Integration for V2 X Security
 - 3.13.6 Homomorphic Encryption Applications
 - 3.13.7 Biometric Authentication Integration
 - 3.13.8 Security-as-a-Service Models
- 3.14 Autonomous Vehicle Security Integration
 - 3.14.1 SAE level-specific security requirements
 - 3.14.2 Multi-level security coordination
 - 3.14.3 Human-machine interface security
 - 3.14.4 Fail-safe security mechanisms
 - 3.14.5 Remote operation security
 - 3.14.6 Fleet security management
 - 3.14.7 Edge case security handling
- 3.15 V2X security testing & validation
 - 3.15.1 Security testing methodology
 - 3.15.2 Penetration testing requirements
 - 3.15.3 Vulnerability assessment processes
 - 3.15.4 Real-world attack simulation
 - 3.15.5 Compliance testing frameworks
 - 3.15.6 Continuous security monitoring
 - 3.15.7 Third-party security validation

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 AUTONOMY INTEGRATION, 2021-2034 (\$BN, UNITS)

- 5.1 Key trends
- 5.2 Hardware Security Module (HSM)
- 5.3 Trusted Platform Module (TPM)
- 5.4 Crypto accelerators (on-chip)
- 5.5 Root of Trust
- 5.6 Secure microcontrollers or secure SoCs

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

- 6.1 Key trends
- 6.2 Discrete Security Chips
- 6.3 Integrated Security Solutions
- 6.4 Software-Defined Security
- 6.5 Hybrid Security Architectures
- 6.6 Quantum-Ready Security Chips

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

- 7.1 Key trends

- 7.2 Vehicle-to-Vehicle (V2V)
- 7.3 Vehicle-to-Infrastructure (V2I)
- 7.4 Vehicle-to-Pedestrian (V2P)
- 7.5 Vehicle-to-Network (V2N)
- 7.6 Vehicle-to-Device (V2D)

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

- 8.1 Key trends
- 8.2 Passenger cars
 - 8.2.1 Hatchbacks
 - 8.2.2 Sedans
 - 8.2.3 SUVs
 - 8.2.4 MPVs
- 8.3 Commercial vehicles
 - 8.3.1 Light commercial vehicles (LCVs)
 - 8.3.2 Medium commercial vehicles (MCVs)
 - 8.3.3 Heavy commercial vehicles (HCVs)

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

- 9.1 Key trends
- 9.2 Safety & Collision Avoidance
- 9.3 Traffic Management
- 9.4 Infotainment
- 9.5 Navigation & Routing
- 9.6 Remote Diagnostics
- 9.7 Fleet Management

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

- 10.1 Key trends
- 10.2 OEM
- 10.3 Aftermarket

CHAPTER 11 MARKET ESTIMATES & FORECAST, BY REGION, 2021 - 2034 (\$BN,

UNITS)

- 11.1 Key trends
- 11.2 North America
 - 11.2.1 US
 - 11.2.2 Canada
- 11.3 Europe
 - 11.3.1 Germany
 - 11.3.2 UK
 - 11.3.3 France
 - 11.3.4 Italy
 - 11.3.5 Spain
 - 11.3.6 Russia
 - 11.3.7 Nordics
- 11.4 Asia Pacific
 - 11.4.1 China
 - 11.4.2 India
 - 11.4.3 Japan
 - 11.4.4 Australia
 - 11.4.5 South Korea
 - 11.4.6 Philippines
 - 11.4.7 Indonesia
- 11.5 Latin America
 - 11.5.1 Brazil
 - 11.5.2 Mexico
 - 11.5.3 Argentina
- 11.6 MEA
 - 11.6.1 South Africa
 - 11.6.2 Saudi Arabia
 - 11.6.3 UAE

CHAPTER 12 COMPANY PROFILES

- 12.1 Global Players
 - 12.1.1 Bosch
 - 12.1.2 Broadcom
 - 12.1.3 Continental
 - 12.1.4 Denso
 - 12.1.5 Infineon

- 12.1.6 Marvell Technology
- 12.1.7 NXP Semiconductors
- 12.1.8 Qualcomm Technologies
- 12.1.9 Renesas Electronics
- 12.1.10 STMicroelectronics
- 12.1.11 Texas Instruments
- 12.2 Regional Players
 - 12.2.1 Analog Devices
 - 12.2.2 Giesecke+Devrient Mobile Security
 - 12.2.3 Huawei
 - 12.2.4 IDEMIA
 - 12.2.5 MediaTek
 - 12.2.6 On Semiconductor
 - 12.2.7 Rohm Semiconductor
 - 12.2.8 Samsung
- 12.3 Emerging Players
 - 12.3.1 Aptiv
 - 12.3.2 Autotalks
 - 12.3.3 Cohda Wireless
 - 12.3.4 Commsignia
 - 12.3.5 Escrypt
 - 12.3.6 Ficos
 - 12.3.7 Inside Secure
 - 12.3.8 Microchip Technology
 - 12.3.9 Rambus
 - 12.3.10 Secure-IC S.A.S.

I would like to order

Product name: Vehicle-to-everything (V2X) Security Chips Market Opportunity, Growth Drivers, Industry Trend Analysis, and Forecast 2025 - 2034

Product link: <https://marketpublishers.com/r/V1EF420D2F09EN.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/V1EF420D2F09EN.html>