

**Connected Car Security Market by Type (Endpoint, Application, Network, Security),  
Solution (Software & Hardware), Application (TCU, Infotainment, ADAS,  
Communication Modules), Form (In-vehicle, External Cloud), EV Type & Region -  
Global Forecast to 2032**

Market Report | 2025-12-05 | 278 pages | MarketsandMarkets

**AVAILABLE LICENSES:**

- Single User \$4950.00
- Multi User \$6650.00
- Corporate License \$8150.00
- Enterprise Site License \$10000.00

**Report description:**

The connected car security market is projected to grow from USD 3.37 billion in 2025 to reach USD 6.99 billion by 2032, at a CAGR of 11.0% from 2025 to 2032. Market growth is driven by the rapid expansion of software-defined vehicles (SDVs), over-the-air (OTA) update capabilities, V2X communication, and the rising cybersecurity threats targeting vehicle ECUs, telematics units, and cloud platforms. Additionally, regulations such as UNECE WP.29 CSMS, ISO/SAE 21434, the US NHTSA cybersecurity guidelines, and China's Automotive Data Security Regulations are pushing automakers to adopt secure gateways, IDS/IPS, hardware-secured modules, and encrypted communication frameworks. Moreover, the shift toward electric vehicles and connected ADAS features increases cybersecurity complexity, requiring multi-layer protection for infotainment, telematics, and autonomous driving stacks. Substantial contributions from the Asia Pacific region, especially China, combined with increasing investments from Europe and North America, are accelerating the global adoption of advanced connected car security architectures.

<https://mnmimg.marketsandmarkets.com/Images/connected-car-security-market-img-overview.webp>

"By form, the in-vehicle solutions segment is projected to account for a larger share than the external cloud services segment during the forecast period."

The dominance of in-vehicle security solutions is driven by the rising complexity of electronic control units (ECUs), domain controllers, and telematics systems, which require embedded protection to prevent unauthorized access and system manipulation. Compliance mandates under UNECE WP.29, ISO/SAE 21434, and China's Automotive Data Security Regulations have

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

accelerated OEM adoption of secure gateways, hardware security modules (HSMs), and intrusion detection systems inside the vehicle architecture. As connected ADAS, digital cockpits, and V2X communication become standard across mid-range and premium models, in-vehicle security becomes the core protection layer for safeguarding internal networks, OTA software, and data flows. This sustained regulatory and technological push positions in-vehicle solutions as the largest revenue-generating segment in the market.

?

"By solution type, the hardware-based solutions segment is projected to be a faster-growing segment than the software-based segment during the forecast period."

The use of hardware-based solutions is expanding rapidly due to the industry's shift toward tamper-resistant architectures that ensure secure data processing, cryptographic key storage, and real-time threat mitigation at the ECU level. Components such as TPMs, HSMs, secure microcontrollers, and cryptographic accelerators are becoming essential for protecting safety-critical ADAS systems, high-performance computing units, and autonomous driving platforms. With rising cybersecurity threats targeting vehicle firmware and communication buses, OEMs are increasingly adopting hardware-rooted trust models for stronger authentication and encryption. Growing SDV adoption and the need for secured zonal architectures further accelerate demand, making hardware-based solutions the fastest-growing segment despite higher integration costs.

"Asia Pacific is projected to be the fastest-growing segment in the global connected car security market during the forecast period."

Asia Pacific is projected to witness strong and accelerating growth driven by the rapid expansion of connected and autonomous mobility ecosystems in China, Japan, South Korea, and India. China is leading this momentum through the strict enforcement of the automotive data security regulations, compelling OEMs such as BYD, NIO, XPeng, Zeekr, and SAIC to adopt encrypted in-vehicle communication, secure OTA platforms, and embedded IDS/IPS solutions. Japan and South Korea are advancing deployments in line with UNECE WP.29 CSMS frameworks, supported by robust telematics networks and high connected car penetration across both luxury and mass-market segments. With rapid EV adoption, strong 5G rollout, and government-led cybersecurity compliance, Asia Pacific continues to generate significant new revenue opportunities, making it the fastest-growing region in the connected car security market.

In-depth interviews were conducted with CEOs, marketing directors, other innovation and technology directors, and executives from various key organizations operating in this market.

-□By Company Type: OEMs - 10% and Tier 1 Companies - 90%

-□By Designation: C-Level Executive - 60%; Director-Level - 30%; Others - 10%

-□By Region: North America - 40%; Europe - 50%; and Asia Pacific - 10%

Note: Others include Sales Managers and Product Managers.

The connected car security market is dominated by major players, such as NXP Semiconductors (Netherlands), AUMOVIO SE (Germany), Harman International (US), Vector Informatik GmbH (Germany), BlackBerry Limited (Canada), Thales (France), ARM Limited (UK), WirelessCar (Sweden), Astemo Ltd. (Japan), and Keysight Technologies (US). These companies are expanding their portfolios to strengthen their connected car security market position.

#### Research Coverage

The report covers the connected car security market in terms of security type (Endpoint Security, Application Security, Network Security, and Cloud Security), application [Telematics Control Units (TCUs), Infotainment Systems, ADAS & Autonomous Driving Systems, and Communication Modules], electric vehicle type (BEV, PHEV, HEV, and FCEV), solution type (Software-based Solutions and Hardware-based Solutions), form (In-Vehicle Solutions and External Cloud Services), and Region (North America, Asia Pacific, Europe, and Rest of the World). It covers the competitive landscape and company profiles of the key players in the significant connected car security market.

The study also includes an in-depth competitive analysis of the key market players, their company profiles, key observations related to product and business offerings, recent developments, and key market strategies.

#### Key Benefits of Buying the Report:

-□The report will help market leaders/new entrants with information on the closest approximations of revenue numbers for the

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

connected car security market and its subsegments.

-□ This report will help stakeholders understand the competitive landscape and gain more insights, enabling them to position their businesses better and plan suitable go-to-market strategies.

-□ The report will also help stakeholders understand the market pulse and provide information on key market drivers, restraints, challenges, and opportunities.

-□ The report will also help stakeholders understand the current and future pricing trends of the connected car security market.

The report also provides insights into the following pointers:

-□ Analysis of key drivers (Increasing vehicle connectivity through telematics and V2X, mandatory compliance with global automotive cybersecurity regulations, and rising cyberattacks on connected and autonomous vehicles), restraints (Legacy ECU and vehicle architectures complicate security upgrades and high implementation and integration costs), opportunities (Growth of managed security services and vehicle SOCs, rising demand for secure OTA and lifecycle management, and V2X and 5G networks requiring strong PKI-based security), and challenges (Evolving cyber threats and minimizing false positives without compromising safety-critical functions)

-□ Product Developments/Innovation: Detailed insights into upcoming technologies, research & development activities, and product & service launches in the connected car security market.

-□ Market Development: Comprehensive information about lucrative markets across varied regions

-□ Market Diversification: Exhaustive information about new products & services, untapped geographies, recent developments, and investments in the connected car security market

-□ Competitive Assessment: In-depth assessment of market share, growth strategies, and service offerings of leading players like as NXP Semiconductors (Netherlands), AUMOVIO SE (Germany), Harman International (US), Vector Informatik GmbH (Germany), BlackBerry Limited (Canada), Thales (France), ARM Limited (UK), WirelessCar (Sweden), Astemo Ltd. (Japan), and Keysight Technologies (US), among others, in connected car security market

## **Table of Contents:**

1	INTRODUCTION	25
1.1	STUDY OBJECTIVES	25
1.2	MARKET DEFINITION	25
1.3	STUDY SCOPE	26
1.3.1	MARKET SEGMENTATION & REGIONAL SCOPE	26
1.3.2	INCLUSIONS & EXCLUSIONS	26
1.4	YEARS CONSIDERED	27
1.5	CURRENCY CONSIDERED	27
1.6	STAKEHOLDERS	27
2	RESEARCH METHODOLOGY	28
2.1	RESEARCH DATA	28
2.1.1	SECONDARY DATA	29
2.1.1.1	Key secondary sources	30
2.1.1.2	Key data from secondary sources	31
2.1.2	PRIMARY DATA	31
2.1.2.1	Primary participants	33
2.1.2.2	Key industry insights	33
2.2	MARKET BREAKDOWN & DATA TRIANGULATION	33
2.3	MARKET SIZE ESTIMATION	34
2.3.1	TOP-DOWN APPROACH	35
2.4	MARKET FORECAST	36
2.5	RESEARCH ASSUMPTIONS	37
2.6	RESEARCH LIMITATIONS	38

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

3	EXECUTIVE SUMMARY	39
3.1	KEY INSIGHTS AND MARKET HIGHLIGHTS	39
3.2	KEY MARKET PARTICIPANTS: SHARED INSIGHTS AND STRATEGIC DEVELOPMENTS	40
3.3	DISRUPTIVE TRENDS SHAPING MARKET	42
3.4	HIGH-GROWTH SEGMENTS AND EMERGING FRONTIERS	43
3.5	SNAPSHOT: GLOBAL MARKET SIZE, GROWTH RATE, AND FORECAST	44
4	PREMIUM INSIGHTS	45
4.1	ATTRACTIVE OPPORTUNITIES FOR PLAYERS IN CONNECTED CAR SECURITY MARKET	45
4.2	CONNECTED CAR SECURITY MARKET, BY SECURITY TYPE	45
4.3	CONNECTED CAR SECURITY MARKET, BY ELECTRIC VEHICLE TYPE	46
4.4	CONNECTED CAR SECURITY MARKET, BY FORM	46
4.5	CONNECTED CAR SECURITY MARKET, BY APPLICATION	47
4.6	CONNECTED CAR SECURITY MARKET, BY SOLUTION TYPE	47
4.7	CONNECTED CAR SECURITY MARKET, BY REGION	48
5	MARKET OVERVIEW	49
5.1	INTRODUCTION	49
5.2	MARKET DYNAMICS	50
5.2.1	DRIVERS	50
5.2.1.1	Increasing vehicle connectivity through telematic and V2X	50
5.2.1.2	Mandatory compliance with global automotive cybersecurity regulations	51
5.2.1.3	Rising cyberattacks on connected and autonomous vehicles	52
5.2.2	RESTRAINTS	53
5.2.2.1	Legacy ECU and vehicle architectures complicating security upgrades	53
5.2.2.2	High implementation and integration costs	53
5.2.3	OPPORTUNITIES	54
5.2.3.1	Growth of managed security services and vehicle SOC's	54
5.2.3.2	Rising demand for secure OTA and lifecycle management	54
5.2.3.3	V2X and 5G networks require strong PKI-based security	55
5.2.4	CHALLENGES	55
5.2.4.1	Evolving cyber threats hindering long-term protection	55
5.2.4.2	Minimizing false positives without compromising safety-critical functions	56
5.3	UNMET NEEDS AND WHITE SPACES	57
5.3.1	UNMET NEEDS IN CONNECTED CAR SECURITY MARKET	57
5.3.2	WHITE SPACE OPPORTUNITIES	57
5.4	INTERCONNECTED MARKETS AND CROSS-SECTOR OPPORTUNITIES	58
5.4.1	INTERCONNECTED MARKETS	58
5.4.2	CROSS-SECTOR OPPORTUNITIES	58
5.5	STRATEGIC MOVES BY TIER 1/2/3 PLAYERS	59
5.5.1	KEY MOVES AND STRATEGIC FOCUS	59
6	INDUSTRY TRENDS	60
6.1	PORTER'S FIVE FORCES ANALYSIS	60
6.1.1	THREAT FROM NEW ENTRANTS	61
6.1.2	THREAT FROM SUBSTITUTES	61
6.1.3	BARGAINING POWER OF SUPPLIERS	61
6.1.4	BARGAINING POWER OF BUYERS	62
6.1.5	INTENSITY OF COMPETITIVE RIVALRY	62
6.2	MACROECONOMIC OUTLOOK	62

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

6.2.1	INTRODUCTION	62
6.2.2	GDP TRENDS AND FORECAST	63
6.2.3	TRENDS IN GLOBAL CONNECTED CAR INDUSTRY	63
6.2.3.1	Transition toward software-defined vehicle era	63
6.2.3.2	Connectivity as enabler of autonomous mobility	64
6.2.3.3	Vehicle-to-everything (V2X) to build foundation for smart mobility	64
6.2.3.4	Evolution of vehicle architecture in software-driven era	65
6.2.3.5	Personalization and connected experiences in modern mobility	65
6.2.4	TRENDS IN GLOBAL AUTOMOTIVE & TRANSPORTATION INDUSTRY	65
6.2.4.1	Rapid but uneven EV adoption and market share gains	65
6.2.4.2	Battery pack cost decline and cell supply overcapacity reshaping economics	66
6.2.4.3	Heavy-duty and commercial electrification (plus selective hydrogen use) accelerating heterogeneously	66
6.2.4.4	ADAS proliferation and measured progress toward high autonomy and rise of pilot robotaxi deployment	67
6.2.4.5	Semiconductor cycles, supply resilience, and industrial policy reshaping auto supply chains	67
6.3	SUPPLY CHAIN ANALYSIS	68
6.4	ECOSYSTEM ANALYSIS	69
6.5	PRICING ANALYSIS	72
6.5.1	INDICATIVE PRICING, BY APPLICATION	72
6.5.2	INDICATIVE PRICING, BY SECURITY TYPE	72
6.5.3	INDICATIVE PRICING, BY REGION	73
6.6	TRADE ANALYSIS	73
6.6.1	IMPORT SCENARIO	73
6.6.2	EXPORT SCENARIO	75
6.7	KEY CONFERENCES & EVENTS, 2025-2026	76
6.8	TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS	76
6.9	INVESTMENT & FUNDING SCENARIO	77
6.10	CASE STUDY ANALYSIS	78
6.10.1	CONTINENTAL DEVELOPED IN-VEHICLE CYBERSECURITY FRAMEWORK TO PROTECT CONNECTED ECUS AND SECURE DATA EXCHANGE	78
6.10.2	BOSCH IMPLEMENTED SECURE GATEWAY MODULE TO CONTROL EXTERNAL ACCESS AND STRENGTHEN VEHICLE COMMUNICATION SECURITY	79
6.10.3	HARMAN ENABLED CLOUD-BASED THREAT DETECTION TO MONITOR AND MITIGATE CYBER RISKS IN CONNECTED VEHICLE FLEETS	79
6.10.4	APTIV DEPLOYED END-TO-END CYBERSECURITY ARCHITECTURE TO SAFEGUARD OVER-THE-AIR UPDATES AND DATA TRANSFER	80
6.10.5	NXP INTRODUCED AUTOMOTIVE HARDWARE SECURITY MODULES TO ENCRYPT DATA AND ENSURE SECURE ECU COMMUNICATION	80
6.10.6	UPSTREAM SECURED VEHICLE FLEET OPERATIONS USING CLOUD ANALYTICS FOR THREAT DETECTION AND INCIDENT RESPONSE	81
6.10.7	ARGUS DEVELOPED NETWORK INTRUSION DETECTION AND PREVENTION SYSTEMS TO IDENTIFY AND BLOCK MALICIOUS TRAFFIC	81
6.10.8	BLACKBERRY QNX PROVIDED SECURE OPERATING SYSTEM FOUNDATION TO SUPPORT SAFETY-CRITICAL AUTOMOTIVE SOFTWARE	82
6.11	US 2025 TARIFF	82
6.11.1	INTRODUCTION	82
6.11.2	KEY TARIFF RATES	83
6.11.2.1	Key product-related tariffs	84

6.11.3	PRICE IMPACT ANALYSIS	84
6.11.4	IMPACT ON COUNTRY/REGION	85
6.11.4.1	US	85
6.11.4.2	Europe	86
6.11.4.3	Asia Pacific	86
6.11.5	IMPACT ON END-USE INDUSTRIES	86
7	CUSTOMER LANDSCAPE AND BUYER BEHAVIOR	88
7.1	DECISION-MAKING PROCESS	88
7.2	BUYER STAKEHOLDERS AND BUYING EVALUATION CRITERIA	89
7.2.1	KEY STAKEHOLDERS IN BUYING PROCESS	89
7.2.2	BUYING CRITERIA	90
7.3	ADOPTION BARRIERS AND INTERNAL CHALLENGES	91
7.4	UNMET NEEDS IN VARIOUS END-USER INDUSTRIES	92
7.5	MARKET PROFITABILITY	92
7.6	REVENUE POTENTIAL	93
7.7	COST DYNAMICS	93
7.8	MARGIN OPPORTUNITIES IN KEY APPLICATIONS	93
8	STRATEGIC DISRUPTION THROUGH TECHNOLOGY, PATENTS, DIGITAL, AND AI ADOPTION	94
8.1	PATENT ANALYSIS	94
8.1.1	INTRODUCTION	94
8.1.2	LIST OF PATENTS GRANTED TO LG ELECTRONICS	98
8.1.3	LIST OF PATENTS GRANTED TO INTEL CORPORATION	99
8.1.4	LIST OF PATENTS GRANTED TO SAMSUNG ELECTRONICS	100
8.2	IMPACT OF GENERATIVE AI ON CONNECTED CAR SECURITY MARKET	101
8.3	KEY EMERGING TECHNOLOGIES	102
8.3.1	VEHICLE SECURITY OPERATIONS CENTERS (VSOCs)	102
8.3.2	INTRUSION DETECTION & PREVENTION SYSTEMS	103
8.3.3	SECURE COMMUNICATION PROTOCOLS	103
8.3.4	ENCRYPTION & CRYPTOGRAPHY	103
8.3.5	HARDWARE SECURITY MODULES (HSMS)	104
8.3.6	TRUSTED PLATFORM MODULES (TPMS)	104
8.3.7	IDENTITY & ACCESS MANAGEMENT (IAM)	105
8.4	COMPLEMENTARY TECHNOLOGIES	105
8.4.1	CLOUD & EDGE-BASED VEHICLE SECURITY	105
8.4.2	AI-/ML-DRIVEN INTRUSION DETECTION & RESPONSE	106
8.4.3	BLOCKCHAIN FOR V2X AND DATA INTEGRITY	107
8.4.4	BIOMETRIC AUTHENTICATION FOR DRIVER & VEHICLE ACCESS	107
?		
8.5	TECHNOLOGY/PRODUCT ROADMAP	108
8.5.1	SHORT-TERM (2025-2027): FOUNDATION & EARLY COMMERCIALIZATION	108
8.5.2	MID-TERM (2027-2030): EXPANSION & STANDARDIZATION	108
8.5.3	LONG-TERM (2030 ONWARDS): MASS COMMERCIALIZATION & DISRUPTION	108
8.6	TECHNOLOGICAL DEVELOPMENTS IN CONNECTED CAR MARKET, BY OEM	109
9	REGULATORY LANDSCAPE	111
9.1	REGULATORY LANDSCAPE	111
9.1.1	REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	111

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

9.2	REGULATIONS, BY REGION	115
9.2.1	NORTH AMERICA	115
9.2.2	EUROPE	116
9.2.3	ASIA PACIFIC	117
10	CONNECTED CAR SECURITY MARKET, BY APPLICATION	118
10.1	INTRODUCTION	118
10.2	TELEMATICS CONTROL UNITS (TCUS)	119
10.2.1	GROWING INTEGRATION OF CONNECTED SERVICES AND REAL-TIME VEHICLE MONITORING TO DRIVE MARKET	119
10.3	INFOTAINMENT SYSTEMS	120
10.3.1	GROWING COMPLEXITY OF INFOTAINMENT ARCHITECTURES TO DRIVE MARKET	120
10.4	ADAS & AUTONOMOUS DRIVING SYSTEMS	122
10.4.1	NEED FOR STRENGTHENING CYBERSECURITY FOR ADAS AND AUTONOMOUS DRIVING SYSTEMS TO BOOST MARKET	122
10.5	COMMUNICATION MODULES	123
10.5.1	GROWING ADOPTION OF OVER-THE-AIR UPDATES, REMOTE DIAGNOSTICS, PREDICTIVE MAINTENANCE, AND CONNECTED-SERVICE PLATFORMS TO DRIVE MARKET	123
11	CONNECTED CAR SECURITY MARKET, BY ELECTRIC VEHICLE TYPE	125
11.1	INTRODUCTION	125
11.2	BEV	126
11.2.1	STRONG ENDPOINT PROTECTION AND SECURE COMMUNICATION FRAMEWORKS IN BEVS TO DRIVE MARKET	126
11.3	PHEV	127
11.3.1	EXPANDING SOFTWARE DEPENDENCIES INCREASING CYBERSECURITY EXPOSURE TO DRIVE MARKET	127
11.4	HEV	129
11.4.1	FOCUS ON SAFEGUARDING VEHICLE-TO-VEHICLE AND VEHICLE-TO-INFRASTRUCTURE CHANNELS TO BOOST MARKET	129
11.5	FCEV	130
11.5.1	RELIANCE OF FCEVS ON CLOUD-BASED INFRASTRUCTURE TO BOOST MARKET	130
12	CONNECTED CAR SECURITY MARKET, BY FORM	132
12.1	INTRODUCTION	132
12.2	IN-VEHICLE SOLUTIONS	133
12.2.1	RAPIDLY ADOPTING ADVANCED ENDPOINT PROTECTION, INTRUSION DETECTION, SECURE UPDATES, AND RESILIENT COMMUNICATION FRAMEWORKS TO DRIVE MARKET	133
12.3	EXTERNAL CLOUD SERVICES	134
12.3.1	INCREASING RELIANCE OF VEHICLES ON ELECTRONIC CONTROL UNITS AND TELEMATICS TO DRIVE MARKET	134
13	CONNECTED CAR SECURITY MARKET, BY SECURITY TYPE	136
13.1	INTRODUCTION	136
13.2	ENDPOINT SECURITY	137
13.2.1	FOCUS ON DEVICE AUTHENTICATION, INTRUSION DETECTION, ENCRYPTION, AND DATA INTEGRITY TO BOOST MARKET	137
13.3	APPLICATION SECURITY	138
13.3.1	NEED FOR SECURING APPLICATIONS AGAINST DATA BREACHES TO DRIVE MARKET	138
13.4	NETWORK SECURITY	140
13.4.1	NEED FOR INTEGRATION OF ADVANCED ENCRYPTION, INTRUSION DETECTION SYSTEMS, AND SECURE GATEWAYS TO BOOST MARKET	140
13.5	CLOUD SECURITY	141
13.5.1	INCREASED RELIANCE OF CONNECTED VEHICLES ON CLOUD FOR OTA UPDATES AND REAL-TIME NAVIGATION TO DRIVE MARKET	141
14	CONNECTED CAR SECURITY MARKET, BY SOLUTION TYPE	143
14.1	INTRODUCTION	143
14.2	SOFTWARE-BASED SOLUTIONS	144

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

14.2.1	POPULARITY OF TELEMATICS, CLOUD CONNECTIVITY, ADAS, AND V2X COMMUNICATION TO BOOST GROWTH	144
14.3	HARDWARE-BASED SOLUTIONS	145
14.3.1	NEED FOR PREVENTING UNAUTHORIZED ACCESS, TAMPERING, AND SYSTEM MANIPULATION TO BOOST MARKET	145
15	CONNECTED CAR SECURITY MARKET, BY REGION	147
15.1	INTRODUCTION	148
15.2	ASIA PACIFIC	149
15.2.1	ASIA PACIFIC: MACROECONOMIC OUTLOOK	150
15.2.2	CHINA	154
15.2.2.1	Enforcement of stringent data rules for connected vehicles to drive market	154
15.2.3	JAPAN	155
15.2.3.1	Focus on strengthening connected car security amid digital shift to boost market	155
	?	
15.2.4	INDIA	157
15.2.4.1	Need for fast-track cybersecurity compliance for connected mobility to boost demand	157
15.2.5	SOUTH KOREA	159
15.2.5.1	Emphasis on enforcing stringent data rules for connected vehicles to boost market	159
15.2.6	REST OF ASIA PACIFIC	161
15.3	EUROPE	163
15.3.1	EUROPE: MACROECONOMIC OUTLOOK	163
15.3.2	UK	166
15.3.2.1	Need for new cybersecurity standards for connected vehicles to boost market	166
15.3.3	GERMANY	168
15.3.3.1	Focus on enforcing CSMS & SUMS compliance for new vehicles to drive market	168
15.3.4	FRANCE	170
15.3.4.1	Stringent enforcement of UNECE cybersecurity requirements to boost market	170
15.3.5	SPAIN	172
15.3.5.1	Innovation and rapid technological advancements to drive market	172
15.3.6	ITALY	173
15.3.6.1	Need for accelerating cybersecurity integration in smart mobility to drive market	173
15.3.7	REST OF EUROPE	175
15.4	NORTH AMERICA	177
15.4.1	NORTH AMERICA: MACROECONOMIC OUTLOOK	177
15.4.2	US	181
15.4.2.1	Focus on strengthening national security rules to drive market	181
15.4.3	CANADA	183
15.4.3.1	Need for advancing security of connected vehicles through comprehensive guidance to boost market	183
15.4.4	MEXICO	184
15.4.4.1	Awareness regarding critical importance of cybersecurity in automotive industry to drive market	184
15.5	REST OF THE WORLD	186
15.5.1	REST OF THE WORLD: MACROECONOMIC OUTLOOK	186
15.5.2	IRAN	189
15.5.2.1	Focus on secure connectivity to drive demand	189
15.5.3	SOUTH AFRICA	191
15.5.3.1	Rising adoption of connected mobility to drive market	191
	?	
16	COMPETITIVE LANDSCAPE	193
16.1	KEY PLAYER STRATEGIES/RIGHT TO WIN, 2022-2024	193

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



16.2	MARKET SHARE ANALYSIS, 2024	195
16.3	REVENUE ANALYSIS, 2020-2024	197
16.4	BRAND COMPARISON	198
16.5	COMPANY VALUATION AND FINANCIAL METRICS	199
16.6	COMPANY EVALUATION MATRIX: KEY PLAYERS, 2024	200
16.6.1	STARS	200
16.6.2	EMERGING LEADERS	200
16.6.3	PERVASIVE PLAYERS	200
16.6.4	PARTICIPANTS	201
16.6.5	COMPANY FOOTPRINT: KEY PLAYERS, 2024	202
16.6.5.1	Company footprint	202
16.6.5.2	Region footprint	202
16.6.5.3	Solution type footprint	203
16.6.5.4	Security type footprint	205
16.7	COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2024	206
16.7.1	PROGRESSIVE COMPANIES	206
16.7.2	RESPONSIVE COMPANIES	206
16.7.3	DYNAMIC COMPANIES	206
16.7.4	STARTING BLOCKS	206
16.7.5	COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2024	208
16.7.5.1	Detailed list of key startups/SMEs	208
16.7.5.2	Competitive benchmarking of key startups/SMEs	209
16.8	COMPETITIVE SCENARIO	210
16.8.1	PRODUCT LAUNCHES/ENHANCEMENTS	210
16.8.2	DEALS	211
17	COMPANY PROFILES	215
17.1	KEY PLAYERS	215
17.1.1	AUMOVIO SE	215
17.1.1.1	Business overview	215
17.1.1.2	Products/Solutions/Services offered	216
17.1.1.3	Recent developments	218
17.1.1.3.1	Product launches/enhancements	218
17.1.1.3.2	Deals	218
17.1.1.3.3	Expansion	219
17.1.1.4	MnM view	220
17.1.1.4.1	Key strengths	220
17.1.1.4.2	Strategic choices	220
17.1.1.4.3	Weaknesses and competitive threats	220
	?	
17.1.2	BLACKBERRY LIMITED	221
17.1.2.1	Business overview	221
17.1.2.2	Products/Solutions/Services offered	222
17.1.2.3	Recent developments	223
17.1.2.3.1	Product launches/enhancements	223
17.1.2.3.2	Deals	224
17.1.2.4	MnM view	225
17.1.2.4.1	Key strengths	225

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

17.1.2.4.2	Strategic choices	225
17.1.2.4.3	Weaknesses & competitive threats	225
17.1.3	VECTOR INFORMATIK GMBH	226
17.1.3.1	Business overview	226
17.1.3.2	Products/Solutions/Services offered	226
17.1.3.3	Recent developments	228
17.1.3.3.1	Product launches/enhancements	228
17.1.3.3.2	Deals	228
17.1.3.4	MnM view	229
17.1.3.4.1	Key strengths	229
17.1.3.4.2	Strategic choices	229
17.1.3.4.3	Weaknesses and competitive threats	229
17.1.4	NXP SEMICONDUCTORS	230
17.1.4.1	Business overview	230
17.1.4.2	Products/Solutions/Services offered	231
17.1.4.3	Recent developments	232
17.1.4.3.1	Deals	232
17.1.4.4	MnM view	233
17.1.4.4.1	Key strengths	233
17.1.4.4.2	Strategic choices	233
17.1.4.4.3	Weaknesses and competitive threats	233
17.1.5	HARMAN INTERNATIONAL	234
17.1.5.1	Business overview	234
17.1.5.2	Products/Solutions/Services offered	235
17.1.5.3	Recent developments	235
17.1.5.3.1	Deals	235
17.1.5.4	MnM view	236
17.1.5.4.1	Key strengths	236
17.1.5.4.2	Strategic choices	236
17.1.5.4.3	Weaknesses and competitive threats	237
?		
17.1.6	UPSTREAM SECURITY LTD.	238
17.1.6.1	Business overview	238
17.1.6.2	Products/Solutions/Services offered	238
17.1.6.3	Recent developments	239
17.1.6.3.1	Product launches/enhancements	239
17.1.6.3.2	Deals	239
17.1.7	ASTEMO, LTD.	240
17.1.7.1	Business overview	240
17.1.7.2	Products/Solutions/Services offered	240
17.1.7.3	Recent developments	241
17.1.7.3.1	Deals	241
17.1.7.3.2	Expansion	241
17.1.8	TRUSTONIC	242
17.1.8.1	Business overview	242
17.1.8.2	Products/Solutions/Services offered	242
17.1.8.3	Recent developments	243

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

17.1.8.3.1	Product launches/enhancements	243
17.1.8.3.2	Deals	244
17.1.9	KPIT	245
17.1.9.1	Business overview	245
17.1.9.2	Products/Solutions/Services offered	246
17.1.9.3	Recent developments	247
17.1.9.3.1	Deals	247
17.1.10	THALES	248
17.1.10.1	Business overview	248
17.1.10.2	Products/Solutions/Services offered	249
17.1.10.3	Recent developments	250
17.1.10.3.1	Product launches/enhancements	250
17.1.10.3.2	Deals	250
17.1.11	T-SYSTEMS INTERNATIONAL GMBH	251
17.1.11.1	Business overview	251
17.1.11.2	Products/Solutions/Services offered	251
17.1.11.3	Recent developments	252
17.1.11.3.1	Product launches/enhancements	252
17.1.11.3.2	Deals	253
17.1.12	AUTOCRYPT CO., LTD.	254
17.1.12.1	Business overview	254
17.1.12.2	Products/Solutions/Services offered	254
17.1.12.3	Recent developments	256
17.1.12.3.1	Product launches/enhancements	256
17.1.12.3.2	Deals	257
?		
17.2	OTHER PLAYERS	258
17.2.1	ARM LIMITED	258
17.2.2	TREND MICRO INCORPORATED	259
17.2.3	ETAS	260
17.2.4	KEYSIGHT TECHNOLOGIES	261
17.2.5	INTERTEK GROUP PLC	262
17.2.6	DEVICE AUTHORITY	263
17.2.7	SECUNET SECURITY NETWORKS AG	264
17.2.8	TRILLIUM SECURE, INC.	265
17.2.9	WIRELESSCAR	266
17.2.10	KARAMBA SECURITY	267
17.2.11	INTERTRUST TECHNOLOGIES CORPORATION	268
17.2.12	GUARDKNOX	269
17.2.13	TATA ELXSI	270
18	APPENDIX	271
18.1	DISCUSSION GUIDE	271
18.2	KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL	274
18.3	CUSTOMIZATION OPTIONS	276
18.4	RELATED REPORTS	276
18.5	AUTHOR DETAILS	277

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

**Connected Car Security Market by Type (Endpoint, Application, Network, Security),  
Solution (Software & Hardware), Application (TCU, Infotainment, ADAS,  
Communication Modules), Form (In-vehicle, External Cloud), EV Type & Region -  
Global Forecast to 2032**

Market Report | 2025-12-05 | 278 pages | MarketsandMarkets

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	\$4950.00
	Multi User	\$6650.00
	Corporate License	\$8150.00
	Enterprise Site License	\$10000.00
		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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Zip Code\*

Country\*

Date

Signature