

South Korea IoT Security Market Size, Share, Trends and Forecast by Component, Security Type, Vertical, and Region, 2026-2034

<https://marketpublishers.com/r/S19A12052AA9EN.html>

Date: July 2026

Pages: 122

Price: US\$ 2,999.00 (Single User License)

ID: S19A12052AA9EN

Abstracts

The South Korea IoT security market size reached USD 149.4 Million in 2025. Looking forward, IMARC Group expects the market to reach USD 1,115.1 Million by 2034, exhibiting a growth rate (CAGR) of 24.28% during 2026-2034. The market is driven by strict national regulations that enforce security-by-design practices in IoT systems. Expanding deployment of connected devices across smart factories, healthcare, and energy infrastructure intensifies the need for robust, scalable protection. Rising sophistication of cyber threats is pushing businesses toward proactive risk frameworks, further augmenting the South Korea IoT security market share.

SOUTH KOREA IOT SECURITY MARKET TRENDS:

Proliferation of Connected Devices Across Industries

South Korea's rapid industrial digitization and smart infrastructure development are leading to unprecedented deployment of connected devices across numerous end-use sectors. For instance, on July 8, 2025, South Korea's government unveiled a KRW 27.3 Billion (USD 19.9 Million) initiative to build micro data centers (MDCs) powered by domestically developed AI chips. These MDCs will provide low-latency, cost-effective AI services to SMEs, hospitals, and public institutions, with a focus on regions outside metropolitan areas. Connected healthcare platforms as well as smart systems depend on real-time data flow, making them vulnerable to cyber intrusions. Each connected node, whether a machine sensor, wearable device, or control system, represents a potential entry point for malicious actors. The increasing density of these endpoints creates a pressing need for endpoint detection and response (EDR), identity verification protocols, and encrypted data pathways. Businesses now recognize that IoT security is

not a modular add-on, but a critical foundation of digital resilience.

Manufacturers are embedding secure chipsets and cryptographic modules into devices at the design phase. In the energy and logistics sectors, where system disruption has far-reaching consequences, multi-layered security solutions are being prioritized. These include network segmentation, access control policies, and device monitoring tools. As enterprises scale up automation and data integration across value chains, the exposure to cyber risk grows proportionally. The resulting demand for security solutions tailored to complex, heterogeneous IoT environments is a defining trend of South Korea's cybersecurity landscape and a major contributor to South Korea IoT security market growth.

Evolving Threat Landscape and Strategic Risk Management

The frequency and complexity of cyber threats targeting IoT ecosystems in South Korea have intensified, prompting a shift from reactive defense to proactive risk management. Sophisticated attacks, including ransomware on industrial systems, data interception on consumer devices, and coordinated assaults on public infrastructure, have raised alarm across industries. In response, organizations are moving beyond conventional firewalls and adopting adaptive security strategies involving behavioral analytics, zero-trust frameworks, and continuous authentication. In line with this growing need for advanced security, recent developments highlight the increasing focus on enhancing IoT security infrastructure. On June 22, 2025, SK Group and AWS announced a 15-year partnership to build an AI data center in Ulsan, South Korea, which will strengthen the country's AI and IoT ecosystem. The project is expected to generate up to 78,000 direct and indirect jobs and forms part of AWS's USD 5.88 Billion (approx. 7.85 Trillion won) investment in South Korea by 2027, reflecting a broader industry push toward robust, secure, and scalable cloud infrastructure. There is also increasing adoption of blockchain for securing device identities and AI-driven threat intelligence for anticipating breaches before they occur. Enterprises are developing dedicated IoT security teams and collaborating with external security service providers to design end-to-end protocols that cover device, network, and application layers. Insurance firms have begun linking cyber insurance premiums to the strength of an organization's IoT security posture, further incentivizing investment. Within national defense and telecom sectors, emphasis on cyber hardening has led to increased deployment of quantum-resistant algorithms and advanced anomaly detection systems. This evolving threat environment is no longer a backdrop but a central factor in organizational decision-making. Heightened awareness of strategic risk is transforming IoT security from a technical requirement into a boardroom priority, accelerating momentum in the market.

SOUTH KOREA IOT SECURITY MARKET SEGMENTATION:

IMARC Group provides an analysis of the key trends in each segment of the market, along with forecasts at the country and regional levels for 2026-2034. Our report has categorized the market based on component, security type, and vertical.

Component Insights:

Solutions

Services

The report has provided a detailed breakup and analysis of the market based on the component. This includes solutions and services.

Security Type Insights:

Network Security

Endpoint Security

Application Security

Cloud Security

Others

The report has provided a detailed breakup and analysis of the market based on the security type. This includes network security, endpoint security, application security, cloud security, and others.

Vertical Insights:

Energy and Utilities

Manufacturing

Automotive

Transport

Consumer Electronics

Healthcare

Others

The report has provided a detailed breakup and analysis of the market based on the vertical. This includes energy and utilities, manufacturing, automotive, transport, consumer electronics, healthcare, and others.

Regional Insights:

Seoul Capital Area

Yeongnam (Southeastern Region)

Honam (Southwestern Region)

Hoseo (Central Region)

Others

The report has also provided a comprehensive analysis of all major regional markets. This includes Seoul Capital Area, Yeongnam (Southeastern Region), Honam (Southwestern Region), Hoseo (Central Region), and others.

COMPETITIVE LANDSCAPE:

The market research report has also provided a comprehensive analysis of the competitive landscape. Competitive analysis such as market structure, key player positioning, top winning strategies, competitive dashboard, and company evaluation quadrant has been covered in the report. Also, detailed profiles of all major companies have been provided.

KEY QUESTIONS ANSWERED IN THIS REPORT

How has the South Korea IoT security market performed so far and how will it perform in the coming years?

What is the breakup of the South Korea IoT security market on the basis of component?

What is the breakup of the South Korea IoT security market on the basis of security type?

What is the breakup of the South Korea IoT security market on the basis of vertical?

What is the breakup of the South Korea IoT security market on the basis of region?

What are the various stages in the value chain of the South Korea IoT security market?

What are the key driving factors and challenges in the South Korea IoT security?

What is the structure of the South Korea IoT security market and who are the key players?

What is the degree of competition in the South Korea IoT security market?

Contents

1 PREFACE

2 SCOPE AND METHODOLOGY

- 2.1 Objectives of the Study
- 2.2 Stakeholders
- 2.3 Data Sources
 - 2.3.1 Primary Sources
 - 2.3.2 Secondary Sources
- 2.4 Market Estimation
 - 2.4.1 Bottom-Up Approach
 - 2.4.2 Top-Down Approach
- 2.5 Forecasting Methodology

3 EXECUTIVE SUMMARY

4 SOUTH KOREA IOT SECURITY MARKET - INTRODUCTION

- 4.1 Overview
- 4.2 Market Dynamics
- 4.3 Industry Trends
- 4.4 Competitive Intelligence

5 SOUTH KOREA IOT SECURITY MARKET LANDSCAPE

- 5.1 Historical and Current Market Trends (?2020-2025?)
- 5.2 Market Forecast (?2026-2034?)

6 SOUTH KOREA IOT SECURITY MARKET - BREAKUP BY COMPONENT

- 6.1 Solutions
 - 6.1.1 Overview
 - 6.1.2 Historical and Current Market Trends (?2020-2025?)
 - 6.1.3 Market Forecast (?2026-2034?)
- 6.2 Services
 - 6.2.1 Overview
 - 6.2.2 Historical and Current Market Trends (?2020-2025?)

6.2.3 Market Forecast (?2026-2034?)

7 SOUTH KOREA IOT SECURITY MARKET - BREAKUP BY SECURITY TYPE

7.1 Network Security

7.1.1 Overview

7.1.2 Historical and Current Market Trends (?2020-2025?)

7.1.3 Market Forecast (?2026-2034?)

7.2 Endpoint Security

7.2.1 Overview

7.2.2 Historical and Current Market Trends (?2020-2025?)

7.2.3 Market Forecast (?2026-2034?)

7.3 Application Security

7.3.1 Overview

7.3.2 Historical and Current Market Trends (?2020-2025?)

7.3.3 Market Forecast (?2026-2034?)

7.4 Cloud Security

7.4.1 Overview

7.4.2 Historical and Current Market Trends (?2020-2025?)

7.4.3 Market Forecast (?2026-2034?)

7.5 Others

7.5.1 Historical and Current Market Trends (?2020-2025?)

7.5.2 Market Forecast (?2026-2034?)

8 SOUTH KOREA IOT SECURITY MARKET - BREAKUP BY VERTICAL

8.1 Energy and Utilities

8.1.1 Overview

8.1.2 Historical and Current Market Trends (?2020-2025?)

8.1.3 Market Forecast (?2026-2034?)

8.2 Manufacturing

8.2.1 Overview

8.2.2 Historical and Current Market Trends (?2020-2025?)

8.2.3 Market Forecast (?2026-2034?)

8.3 Automotive

8.3.1 Overview

8.3.2 Historical and Current Market Trends (?2020-2025?)

8.3.3 Market Forecast (?2026-2034?)

8.4 Transport

- 8.4.1 Overview
- 8.4.2 Historical and Current Market Trends (?2020-2025?)
- 8.4.3 Market Forecast (?2026-2034?)
- 8.5 Consumer Electronics
 - 8.5.1 Overview
 - 8.5.2 Historical and Current Market Trends (?2020-2025?)
 - 8.5.3 Market Forecast (?2026-2034?)
- 8.6 Healthcare
 - 8.6.1 Overview
 - 8.6.2 Historical and Current Market Trends (?2020-2025?)
 - 8.6.3 Market Forecast (?2026-2034?)
- 8.7 Others
 - 8.7.1 Historical and Current Market Trends (?2020-2025?)
 - 8.7.2 Market Forecast (?2026-2034?)

8 SOUTH KOREA IOT SECURITY MARKET – BREAKUP BY REGION

- 8.1.1 Seoul Capital Area
 - 8.1.1.1 Overview
 - 8.1.1.2 Historical and Current Market Trends (?2020-2025?)
 - 8.1.1.3 Market Breakup by Component
 - 8.1.1.4 Market Breakup by Security Type
 - 8.1.1.5 Market Breakup by Vertical
 - 8.1.1.6 Key Players
 - 8.1.1.7 Market Forecast (?2026-2034?)
- 8.1.2 Yeongnam (Southeastern Region)
 - 8.1.2.1 Overview
 - 8.1.2.2 Historical and Current Market Trends (?2020-2025?)
 - 8.1.2.3 Market Breakup by Component
 - 8.1.2.4 Market Breakup by Security Type
 - 8.1.2.5 Market Breakup by Vertical
 - 8.1.2.6 Key Players
 - 8.1.2.7 Market Forecast (?2026-2034?)
- 8.1.3 Honam (Southwestern Region)
 - 8.1.3.1 Overview
 - 8.1.3.2 Historical and Current Market Trends (?2020-2025?)
 - 8.1.3.3 Market Breakup by Component
 - 8.1.3.4 Market Breakup by Security Type
 - 8.1.3.5 Market Breakup by Vertical

- 8.1.3.6 Key Players
- 8.1.3.7 Market Forecast (?2026-2034?)
- 8.1.4 Hoseo (Central Region)
 - 8.1.4.1 Overview
 - 8.1.4.2 Historical and Current Market Trends (?2020-2025?)
 - 8.1.4.3 Market Breakup by Component
 - 8.1.4.4 Market Breakup by Security Type
 - 8.1.4.5 Market Breakup by Vertical
 - 8.1.4.6 Key Players
 - 8.1.4.7 Market Forecast (?2026-2034?)
- 8.1.5 Others
 - 8.1.5.1 Historical and Current Market Trends (?2020-2025?)
 - 8.1.5.2 Market Forecast (?2026-2034?)

9 SOUTH KOREA IOT SECURITY MARKET – COMPETITIVE LANDSCAPE

- 9.1 Overview
- 9.2 Market Structure
- 9.3 Market Player Positioning
- 9.4 Top Winning Strategies
- 9.5 Competitive Dashboard
- 9.6 Company Evaluation Quadrant

10 PROFILES OF KEY PLAYERS

- 10.1 Company A
 - 10.1.1 Business Overview
 - 10.1.2 Services Offered
 - 10.1.3 Business Strategies
 - 10.1.4 SWOT Analysis
 - 10.1.5 Major News and Events
- 10.2 Company B
 - 10.2.1 Business Overview
 - 10.2.2 Services Offered
 - 10.2.3 Business Strategies
 - 10.2.4 SWOT Analysis
 - 10.2.5 Major News and Events
- 10.3 Company C
 - 10.3.1 Business Overview

- 10.3.2 Services Offered
- 10.3.3 Business Strategies
- 10.3.4 SWOT Analysis
- 10.3.5 Major News and Events
- 10.4 Company D
 - 10.4.1 Business Overview
 - 10.4.2 Services Offered
 - 10.4.3 Business Strategies
 - 10.4.4 SWOT Analysis
 - 10.4.5 Major News and Events
- 10.5 Company E
 - 10.5.1 Business Overview
 - 10.5.2 Services Offered
 - 10.5.3 Business Strategies
 - 10.5.4 SWOT Analysis
 - 10.5.5 Major News and Events

11 SOUTH KOREA IOT SECURITY MARKET - INDUSTRY ANALYSIS

- 11.1 Drivers, Restraints, and Opportunities
 - 11.1.1 Overview
 - 11.1.2 Drivers
 - 11.1.3 Restraints
 - 11.1.4 Opportunities
- 11.2 Porters Five Forces Analysis
 - 11.2.1 Overview
 - 11.2.2 Bargaining Power of Buyers
 - 11.2.3 Bargaining Power of Suppliers
 - 11.2.4 Degree of Competition
 - 11.2.5 Threat of New Entrants
 - 11.2.6 Threat of Substitutes
- 11.3 Value Chain Analysis

12 APPENDIX

I would like to order

Product name: South Korea IoT Security Market Size, Share, Trends and Forecast by Component, Security Type, Vertical, and Region, 2026-2034

Product link: <https://marketpublishers.com/r/S19A12052AA9EN.html>

Price: US\$ 2,999.00 (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/S19A12052AA9EN.html>