South Korea Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 100 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The South Korea Cybersecurity Market size is estimated at USD 5.06 billion in 2025, and is expected to reach USD 10.18 billion by 2030, at a CAGR of 15.01% during the forecast period (2025-2030).

Cyber threats protect internet-connected systems such as hardware, software, and data. Cybersecurity solutions help enterprises monitor, detect, report, and handle cyber threats to maintain data confidentiality.

Key Highlights
- Owing to the country's increasing number of connected devices, advanced use of mobile devices, and significant intellectual property, South Korea is becoming one of the prime targets for cyber-attacks. Cybersecurity has been prioritized in South Korea's security calculus. The country's cyberspace is at risk because it has not developed an advanced defense-offense cyber capability that has been proven over the last few years. It was subjected to multiple cyber-attacks aimed at critical infrastructure.
- The country is rigorously investing and enhancing its cybersecurity capabilities, which are evident from the fact that it ranked fourth In out of 194 countries in the International Telecommunication Union, ITU Global Cybersecurity Index, 2021. The index consists of the five evaluation categories of law, technology, organization, capability, and cooperation
- South Korea's ICT ministry announced the plan to spend USD 607 million by 2023 to bolster the country's cybersecurity capabilities and respond to growing digital threats. The government plans to develop infrastructure to quickly respond to cybersecurity threats by collaborating with major cloud and data center companies in order to collect threat information in real-time, compared to the current system that relies on individual reports.
- In May 2022, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) signed a Project Arrangement (PA) and Joint Statement of Intent (JSoI), with the Republic of Korea's Ministry of Science and Information Communication Technology (MSIT), for collaborative research, development, and foreign technical exchanges in cybersecurity and

public safety solutions. The effort is part of a Memorandum of Understanding (MoU) signed in 2019 between the two countries in science and technology. The increasing initiatives by the government and the related regulator bodies to prevent such crimes have been increasingly developing or amending rules and regulations. This is expected to fuel the adoption of cybersecurity solutions in the region.
- Moreover, In May 2022, South Korea became the first Asian nation to join NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE). According to the country's National Intelligence Service (NIS), South Korea plans to strengthen its cyber response capabilities by increasing the number of staff sent to the center and expanding the scope of joint training.

South Korea Cyber Security Market Trends

Increasing Cybersecurity incidents is driving the market

- Cybersecurity incidents suspected of originating from North Korea have become increasingly sophisticated in South Korea (Republic of Korea-ROK) by stealing information and millions of dollars, spreading a sense of vulnerability in Korean society. These cyberattacks from North Korea have disrupted information and communications technology (ICT) systems in the ROK government and the country's private sector.
- Incidents of ransomware attacks in South Korea have surged in the past year, shutting hospitals to shopping malls as the coronavirus pandemic led to increased online activities. According to the ICT ministry of South Korea, the country reported 78 ransomware attacks in the first half of 2021.
- In June 2021, South Korea's Nuclear Research Agency, Korea Atomic Energy Research Institute, revealed that their internal networks were hacked by North Korean threat actors using a VPN vulnerability. Such incidents threaten the country and increase the need for cybersecurity solutions across various end-user verticals.
- Moreover, In June 2021, HHM, a South Korean container transportation and shipping company, confirmed that it had detected an unidentified security breach that led to limited access to the e-mail outlook system in certain areas.
- A group of researchers from the Korean Advanced Institute of Science and Technology Constitution (KAIST) based in South Korea identified over 36 mobile security vulnerabilities in LTE mobile data protocol. This makes cybersecurity solutions an essential component and thereby contributing to market growth.

Cloud Deployment Drives the Market Growth

- Many organizations are shifting toward cloud solutions to simplify data storage and provide remote server access on the internet, enabling access to unlimited computing power. Implementing the cloud-based model allows organizations to manage all the applications, providing challenging analytics running in the background.
- Security has been critical at each step of the cloud adoption cycle, as IT provision has moved from on-premise to outside of the company's walls. SMEs prefer cloud deployment as it allows them to focus on their core competencies rather than invest their capital in security infrastructure since they have limited cybersecurity budgets.
- Additionally, the increased adoption of cloud-based email security services is driving the adoption of services integrated with other security platforms, such as IPS and NGFW. This trend is demotivating enterprises to spend on on-premise and dedicated email or web security solutions.
- In March 2022, Alibaba Cloud announced the launch of its first data center in South Korea. The company will offer South Korean customers more secure, reliable, and scalable cloud services, underlining its commitment to empowering South Korean businesses with digital transformation. Such instances will increase the demand for cybersecurity in the country.
- Moreover, In May 2021, Microsoft announced the launch of its first Asia Pacific Public Sector Cyber Security Executive Council

across seven markets in the region, including South Korea. The council aims to accelerate public-private partnerships in cybersecurity, share threat intelligence and build a strong and coordinated response against cyberattacks in the region.

South Korea Cyber Security Industry Overview

The South Korea Cybersecurity Market is highly competitive, with many global players working in the country. These major players adopt strategic initiatives such as mergers and acquisitions, partnerships, and new product offerings due to increasing awareness regarding mobility security among enterprises.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

South Korea Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 100 pages | Mordor Intelligence

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 License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	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*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-01
		Signature