

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

Market Report | 2025-04-28 | 177 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 Saudi Arabia Cybersecurity Market size is estimated at USD 2.19 billion in 2025, and is expected to reach USD 3.67 billion by 2030, at a CAGR of 10.95% during the forecast period (2025-2030).

As online shopping surges, smart gadgets captivate, and cloud technologies gain traction, the market is witnessing a robust growth, driven by escalating cyber threats. With the proliferation of smart devices and IoT technologies, the specter of advancing cyber threats looms larger. In response, businesses are increasingly adopting sophisticated cybersecurity measures, not just to detect and mitigate, but to counteract these threats, further propelling market expansion.

Key Highlights

- Application security focuses on developing, enhancing, and evaluating application features to address security vulnerabilities. Essential protective measures-authentication, encryption, authorization, and logging-aim to prevent unauthorized access, modifications, and anomalies. These safeguards empower enterprises to shield customer data, streamline workflows, and oversee the application lifecycle. In the IT sector, digital transformation and cloud adoption emerge as key catalysts. As companies endeavor to outpace rivals, the emphasis on speed and application security becomes paramount in their digital transformation journey.
- Managed security services encompass a range of solutions, from exposure assessments and detection to security monitoring and operational consulting. MSS providers utilize diverse engagement models, prioritizing both technology and management. As business needs evolve, managed security services have cemented their status as a go-to solution, leading to increased outsourcing advantages for both SMEs and large corporations.
- Saudi Arabia, the Middle East's leading hub for information and communication technology, is in a state of constant evolution. As a pivotal player in the region's growth, the nation is making significant advancements in both infrastructure and technology.

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

- Transitioning from traditional to advanced authentication solutions in cybersecurity may require specialized skills, which current IT teams might lack. This skill deficiency could hinder the adoption of cybersecurity measures, especially in smaller enterprises.

Saudi Arabia Cybersecurity Market Trends

SMEs are Expected to Witness Major Growth

- Saudi Arabia's ongoing investments in digital infrastructure drive SMEs to adopt technology for enhanced operational efficiency and competitiveness. However, due to this digital shift has made them prime targets for cybercriminals. Increasing reports of cyberattacks ranging from ransomware and phishing to data breaches highlight the serious implications for businesses of all sizes. Often perceived as less secure due to their limited resources, SMEs are particularly vulnerable, underscoring the urgent need for effective cybersecurity measures.

- As the number of SMEs increases, business owners are beginning to understand the importance of cyber security. A successful cyberattack can lead to severe financial losses, operational disruptions, and damage to customer trust.

- Further, there has been a growing demand for cybersecurity in the retail sector among SMEs. As e-commerce, digital payments, and online customer interactions surge, retail businesses find themselves increasingly vulnerable to sophisticated cyberattacks. This vulnerability has spurred a notable uptick in the demand for cybersecurity solutions. Historically, large enterprises have been at the forefront of adopting advanced security measures. However, there's a notable shift: SMEs in Saudi Arabia's retail sector now emphasize protecting their operations and data from potential cyber threats.

- The rising demand for cybersecurity solutions among Saudi Arabia's cybersecurity SMEs reflects the evolving digital landscape. As cyber threats grow and regulations tighten, SMEs recognize the need to protect their operations. This awareness, combined with technological advancements and regulatory frameworks, creates opportunities for cybersecurity innovation. By addressing these challenges, Saudi SMEs can safeguard themselves and strengthen their financial position.

Cloud is Expected to Witness Major Growth

- Saudi Arabia's digital transformation, driven by the economic diversification goals of Vision 2030 and a move away from oil dependency, has accelerated in recent years. As the nation increasingly relies on cloud services, both businesses and government entities are placing a premium on cybersecurity. This intensified emphasis on cloud-centric cybersecurity solutions is a direct response to rising cyber threats and the need for agile, effective security measures.

- Furthermore, Saudi Arabian companies are increasingly turning to cloud-based cybersecurity solutions. These cloud platforms enable real-time updates and facilitate the sharing of threat intelligence. Given the ever-evolving nature of cyber threats, staying updated with the latest security measures and threat data is crucial.

- Unlike traditional systems, cloud-based platforms frequently leverage advanced machine learning and artificial intelligence, allowing for more effective threat detection and response.

- As demand surges in Saudi Arabia, numerous companies are unveiling new cloud-based cybersecurity solutions to capture a larger market share. For example, in May 2024, Palo Alto Networks, a US-based cybersecurity provider, unveiled a new cloud location in Saudi Arabia. This strategic move ensures that customers in the Kingdom and the broader region gain local, high-performance access to Palo Alto's premier cybersecurity offerings, aligning with their data residency requirements.

Saudi Arabia Cybersecurity Industry Overview

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

The Saudi Arabian cybersecurity market is fragmented and dominated by a few major players like IBM Corporation, Broadcom Inc., Palo Alto Networks, Trend Micro Inc., and Cisco Systems Inc. These major players, with a prominent share of the market, are focusing on expanding their customer base across foreign countries.

The cybersecurity market comprises several regional and global players in the competitive market space. Although the market poses high barriers to entry for the new players, several new entrants have gained traction.

This market is characterized by moderate/high product differentiation, growing levels of product penetration, and high levels of competition. Generally, the solutions are offered as a package solution, making the consolidated offering look like a part of the product's service.

Many users opt for annual contracts to cut their costs. Lately, companies have also been opting for services that provide faster security updates. This led to increased demand for Cybersecurity solutions, as the updates can be received in real-time. The service-based industry prefers such deployment.

Additional Benefits:

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

Table of Contents:

1 INTRODUCTION

- 1.1 Study Assumptions and Market Definition
- 1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHTS

- 4.1 Market Overview
- 4.2 Industry Attractiveness - Porter's Five Forces Analysis
 - 4.2.1 Bargaining Power of Suppliers
 - 4.2.2 Bargaining Power of Consumers
 - 4.2.3 Threat of New Entrants
 - 4.2.4 Threat of Substitutes
 - 4.2.5 Intensity of Competitive Rivalry
- 4.3 An Assessment of the Impact of Macroeconomic Trends on the Industry

5 MARKET DYNAMICS

- 5.1 Market Drivers
 - 5.1.1 Dynamic Nature of the Security Threats and Strong Investments in the Infrastructural Sector
 - 5.1.2 Shift Toward a Cloud-based Delivery Model
 - 5.1.3 Integration of AI and Other Advanced Technologies
- 5.2 Market Challenges
 - 5.2.1 High Reliance on Traditional Authentication Methods and Low Preparedness
 - 5.2.2 Slow Adoption of Technology in the Oil and Gas Sector in Saudi Arabia

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

- 5.3 Key Use Cases and Case Studies Covering the Highlights of the Problem Statement and Proposed Solution
- 5.4 Regulatory Landscape Covering the Highlights of Regulations Impacting the Adoption of Cybersecurity in the Region
- 5.5 Key Metrics and Indicators
 - 5.5.1 Total Number of Cyberattacks in the Country
 - 5.5.2 Number of Ransomware and Malware Attacks
 - 5.5.3 Delivery Method of Malware and Ransomware Attacks
 - 5.5.4 Cyberattack Trends in Different Industrial Sectors
 - 5.5.5 Average Cost of Cybercrime for Businesses
 - 5.5.6 Most Critical Events of Cyber Attacks in the Country
- 5.6 Technology Landscape
 - 5.6.1 Implication of Zero-trust Architectures to Protect Against Insider Threats
 - 5.6.2 Multi-factor Authentication to Reduce the Risk of Unauthorized Access
 - 5.6.3 Integration of User and Entity Behavioral Analytics to Detect Deviations from Normal Patterns
- 5.7 Cybersecurity Initiatives
 - 5.7.1 National Cybersecurity Strategy
 - 5.7.2 National Cybersecurity Center
 - 5.7.3 Saudi Cybersecurity Higher Education Framework (SCyber-Edu)
 - 5.7.4 Saudi Cybersecurity Workforce Framework (SCyWF)
 - 5.7.5 National Academy of Cybersecurity

6 MARKET SEGMENTATION

- 6.1 By Offering
 - 6.1.1 Solutions
 - 6.1.1.1 Application Security
 - 6.1.1.2 Cloud Security
 - 6.1.1.3 Data Security
 - 6.1.1.4 Identity and Access Management
 - 6.1.1.5 Infrastructure Protection
 - 6.1.1.6 Integrated Risk Management
 - 6.1.1.7 Network Security Equipment
 - 6.1.1.8 End point Security
 - 6.1.1.9 Other Solutions
 - 6.1.2 Services
 - 6.1.2.1 Professional Services
 - 6.1.2.2 Managed Services
- 6.2 By Deployment Mode
 - 6.2.1 Cloud
 - 6.2.2 On-Premise
- 6.3 By Organization Size
 - 6.3.1 SMEs
 - 6.3.2 Large Enterprises
- 6.4 By End User
 - 6.4.1 BFSI
 - 6.4.2 Healthcare
 - 6.4.3 IT and Telecom
 - 6.4.4 Industrial & Defense
 - 6.4.5 Retail

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

- 6.4.6 Energy and Utilities
- 6.4.7 Manufacturing
- 6.4.8 Others

7 COMPETITIVE LANDSCAPE

7.1 Company Profiles

7.1.1 IBM Corporation

7.1.2 Broadcom Inc.

7.1.3 Palo Alto Networks

7.1.4 Trend Micro Inc.

7.1.5 Cisco Systems Inc.

7.1.6 sirar by stc

7.1.7 Taqnia Cyber (Saudi Technology Development and Investment Company (TAQNIA))

7.1.8 EJADA SYSTEMS LTD

7.1.9 Innovative Solutions Co.

7.1.10 Keys Group Services

7.1.11 Alareeb ICT

7.1.12 SAT Microsystems

7.1.13 Saudi Bell Group Company

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

9.1 Upcoming Opportunities in the Market

9.2 Futuristic Technology Trends

9.3 References to Vendor Developments Indicating Futuristic Strategies

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

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

Market Report | 2025-04-28 | 177 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*	<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"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-03-05"/>
		Signature	

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

