Saudi Arabia Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-01-16 | 120 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:

Saudi Arabia Cybersecurity Market Analysis

Saudi Arabia cybersecurity market size in 2026 is estimated at USD 2.42 billion, growing from 2025 value of USD 2.19 billion with 2031 projections showing USD 4.02 billion, growing at 10.66% CAGR over 2026-2031. Strong public-sector spending, mandatory national controls, and rapid cloud migration are the foremost catalysts, while skills shortages and fragmented procurement processes temper overall momentum. Localization mandates are reshaping vendor strategies, with global and local players building joint offerings that blend international technology with Saudi compliance expertise. Government directives around Vision 2030 mega-projects, OT-IT convergence in energy assets, and sovereign cloud initiatives continue to widen the addressable opportunity for advanced threat detection, zero-trust frameworks, and managed security services. Simultaneously, a persistent lack of Saudi nationals with tier-3/4 incident-response expertise is accelerating the shift toward automation and outsourced operations.

Saudi Arabia Cybersecurity Market Trends and Insights

National Cybersecurity Strategy Accelerating Large-Scale SOC and SIEM Deployments

Saudi Arabia's National Cybersecurity Strategy has unlocked record spending on fully staffed security operations centers and enterprise-grade SIEM platforms across ministries and critical agencies. Forty-nine federal bodies now integrate AI into threat-detection workflows, making the Kingdom the regional benchmark for coordinated cyber governance. Standardized

procurement under this program enables volume discounts that favor platform vendors offering end-to-end analytics and incident-response orchestration. Private-sector operators in energy and finance are mirroring these frameworks to remain aligned with federal benchmarks. As a result, AI-enabled monitoring is expected to penetrate 94% of large organizations by 2026, cementing a demand cycle that supports long-term managed-detection-and-response growth.

Mandatory Compliance with NCA Essential Cybersecurity Controls Driving Spending

The updated ECC-2-2024 framework widens mandatory coverage to every entity handling national infrastructure and imposes fixed deadlines for adherence across five governance domains . Procurement timelines have compressed, forcing boards to allocate incremental capital for automated compliance reporting, continuous monitoring, and third-party risk management. Vendors bundling policy templates, control-mapping libraries, and audit-ready dashboards win early contracts, while services revenue accelerates as organizations outsource Governance-Risk-Compliance and red-team assessments.

Shortage of Saudi-Nationals with Tier-3/4 Incident-Response Skills

Despite scholarships and new cyber-academies, demand for forensic talent outstrips supply, lifting salaries by 30-40% in one year and pushing total cost of ownership beyond internal budgets. Enterprises pivot toward managed detection services, AI-augmented triage, and low-code security playbooks to offset the deficit, but knowledge transfer remains an unresolved challenge.

Other drivers and restraints analyzed in the detailed report include:

Hyper-digitization of Vision 2030 Mega-Projects Creating New Attack SurfacesRapid Cloud Migration Post-SDAIA Policy Enabling Saudi-Hosted Public CloudsFragmented Procurement across Semi-Government Entities Slowing Decision Cycles

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Solutions remained the cornerstone of the Saudi Arabia cybersecurity market with a 55.30% revenue contribution in 2025, reflecting mandatory basic-control deployment across ministries and regulated industries. Network firewalls, IAM suites, and endpoint detection platforms formed the bulk of purchases as zero-trust roadmaps matured. Conversely, the Services segment is forecast to expand at an 11.53% CAGR, well above the Saudi Arabia cybersecurity market average of 10.66%. Shortfalls in domestic talent propel outsourcing to managed-security service providers, particularly for 24/7 SOC monitoring and incident response. Professional-services demand also climbs as enterprises seek specialized guidance for ECC audits and OT security architecture.

The paradigm shift toward services is most visible in financial institutions and oil-and-gas operators, where compliance and continuous monitoring are mission-critical. Managed detection and response packages now incorporate AI-driven triage and automated compliance documentation to align with ECC-2-2024 timelines. Vendors offering bundled SOC-as-a-Service with threat-intelligence feeds are capturing mid-market share, while global integrators partner with local firms to address Arabic-language phishing and culturally specific social-engineering vectors.

On-premise deployments held 70.85% of the Saudi Arabia cybersecurity market share in 2025 due to entrenched data-sovereignty preferences and strict residency clauses governing classified workloads. Ministries and refiners continue to favor local appliance-based firewalls and hardened datacenter SIEMs for sensitive applications.

Mission-critical workloads remain on-premise, while analytics, collaboration, and citizen-facing portals migrate to public or

community clouds. This duality drives demand for unified-visibility platforms that correlate telemetry across mixed environments. The Saudi Cloud Computing Company's geographically distributed nodes now deliver integrated WAF, DDoS protection, and workload-encryption services, easing sovereign-cloud adoption for regulated entities and SMEs alike.

Saudi Arabia Cybersecurity Market Report is Segmented by Offering (Solutions [Application Security, Cloud Security, and More], Services [Professional Services, and More]), Deployment Mode (Cloud, On-Premise), End-User Industry (BFSI, Healthcare, IT and Telecom, Government and Defense, Retail and E-Commerce, and More), End-User Enterprise Size (Large Enterprises, Smes). The Market Forecasts are Provided in Terms of Value (USD).

List of Companies Covered in this Report:

IBM Corporation Cisco Systems Inc. Palo Alto Networks, Inc. Fortinet Inc. Broadcom Inc. Trend Micro Inc. sirar by stc Taqnia Cyber EJADA Systems Ltd. Innovative Solutions Co. Keys Group Services Alareeb ICT SAT Microsystems Saudi Bell Group Co. Saudi Information Technology Company (SITE) Check Point Software Technologies Trellix Darktrace plc Elm Company Advanced Electronics Company (AEC) Accenture Security Booz Allen Hamilton

Additional Benefits:

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

Table of Contents:

1 INTRODUCTION
1.1 Market Definition and Study Assumptions
1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET LANDSCAPE
4.1 Market Overview
4.2 Market Drivers
4.2.1 National Cybersecurity Strategy Accelerating Large-Scale SOC and SIEM Deployments
4.2.2 Mandatory Compliance with NCA Essential Cybersecurity Controls (ECC-2018) Driving Spending in Critical Sectors
4.2.3 Hyper-digitisation of Vision 2030 Mega-Projects (NEOM, Red Sea, Qiddiya) Creating New Attack Surfaces
4.2.4 Rapid Cloud Migration Post-SDAIA Policy Enabling Saudi-Hosted Public Clouds
4.2.5 Accelerated OT-ICS Convergence in Oil and Gas and Utilities Boosting Industrial Cybersecurity Demand
4.2.6 Growing Home-grown Talent Pool and Local Content Rules Lowering Procurement Friction for Saudi Vendors
4.3 Market Restraints
4.3.1 Shortage of Saudi-Nationals with Tier-3/4 Incident-Response Skills
4.3.2 Fragmented Procurement across 300+ Semi-Government Entities Slowing Decision Cycles
4.3.3 High Up-front Cost of Zero-Trust Re-architecture for Legacy Ministries
4.3.4 Dependence on Foreign Encryption IP Restricted by Export-Control Licences
4.4 Value Chain Analysis
4.5 Evaluation of Critical Regulatory Framework
4.6 Impact Assessment of Key Stakeholders

4.7 Technological Outlook
4.8 Porter's Five Forces Analysis
4.8.1 Bargaining Power of Suppliers
4.8.2 Bargaining Power of Consumers
4.8.3 Threat of New Entrants
4.8.4 Threat of Substitutes
4.8.5 Intensity of Competitive Rivalry
4.9 Impact of Macro-economic Factors

5 MARKET SIZE AND GROWTH FORECASTS (VALUE)
5.1 By Offering
5.1.1 Solutions
5.1.1.1 Application Security
5.1.1.2 Cloud Security
5.1.1.3 Data Security
5.1.1.4 Identity and Access Management
5.1.1.5 Infrastructure Protection
5.1.1.6 Integrated Risk Management
5.1.1.7 Network Security
5.1.1.8 End-point Security
5.1.2 Services
5.1.2.1 Professional Services
5.1.2.2 Managed Services
5.2 By Deployment Mode
5.2.1 Cloud
5.2.2 On-Premise
5.3 By End-user Industry
5.3.1 BFSI
5.3.2 Healthcare
5.3.3 IT and Telecom
5.3.4 Government and Defense
5.3.5 Retail and E-commerce
5.3.6 Energy and Utilities
5.3.7 Manufacturing
5.3.8 Others
5.4 By End-user Enterprise Size
5.4.1 Large Enterprises
5.4.2 Small and Medium Enterprises (SMEs)

6 COMPETITIVE LANDSCAPE
6.1 Market Concentration
6.2 Strategic Moves
6.3 Market Share Analysis
6.4 Company Profiles (includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share for key companies, Products and Services, and Recent Developments)
6.4.1 IBM Corporation
6.4.2 Cisco Systems Inc.

6.4.3 Palo Alto Networks, Inc.
6.4.4 Fortinet Inc.
6.4.5 Broadcom Inc.
6.4.6 Trend Micro Inc.
6.4.7 sirar by stc
6.4.8 Taqnia Cyber
6.4.9 EJADA Systems Ltd.
6.4.10 Innovative Solutions Co.
6.4.11 Keys Group Services
6.4.12 Alareeb ICT
6.4.13 SAT Microsystems
6.4.14 Saudi Bell Group Co.
6.4.15 Saudi Information Technology Company (SITE)
6.4.16 Check Point Software Technologies
6.4.17 Trellix
6.4.18 Darktrace plc
6.4.19 Elm Company
6.4.20 Advanced Electronics Company (AEC)
6.4.21 Accenture Security
6.4.22 Booz Allen Hamilton

7 MARKET OPPORTUNITIES AND FUTURE TRENDS
7.1 White-space and Unmet-need Assessment

Saudi Arabia Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-01-16 | 120 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	2026-02-09
		Signature	