

Saudi Arabia Intrusion Detection and Prevention Systems Market By Components (Solutions, Services), By Type (Network-Based, Wireless-based, Network behavior analysis, Host-based), By Industry Verticals (Banking, Financial Services and Insurance (BFSI), Government and Defense, Healthcare, Information Technology (IT) and Telecom, Retail and eCommerce, Manufacturing, Others) By Region, Competition, Forecast & Opportunities, 2020-2030F

<https://marketpublishers.com/r/S058AAF42448EN.html>

Date: September 2025

Pages: 86

Price: US\$ 3,500.00 (Single User License)

ID: S058AAF42448EN

Abstracts

Saudi Arabia Intrusion Detection and Prevention Systems (IDPS) Market was valued at USD 174.23 Million in 2024 and is anticipated to reach USD 235.72 million by 2030 with a CAGR of 5.01% through 2030. The Saudi Arabia Intrusion Detection and Prevention Systems market is a rapidly evolving sector that plays a critical role in enhancing the cybersecurity landscape of the Kingdom. As Saudi Arabia embraces digital transformation, advances in technology, and strives to build a knowledge-based economy, the demand for robust IDPS solutions has significantly grown. These systems are instrumental in protecting sensitive data, critical infrastructure, and networks from an expanding array of cyber threats.

With the rising volume and sophistication of cyber threats, the need for enhanced cybersecurity measures is paramount. Organizations across Saudi Arabia recognize that they must safeguard their digital assets to avoid data breaches, financial losses, and damage to their reputation. The IDPS market is driven by the imperative to detect, prevent, and mitigate cyberattacks effectively.

Key Market Drivers

Regulatory & Compliance Mandates

Saudi Arabia has implemented strong regulatory frameworks that directly push enterprises and government bodies to adopt advanced Intrusion Detection & Prevention Systems (IDPS). Financial regulators, energy sector authorities, and the National Cybersecurity Authority (NCA) enforce strict compliance requirements mandating continuous monitoring, logging, and preventive controls. These rules make IDPS not optional but a necessity for regulated organizations.

Banks, for example, must demonstrate preventive measures, continuous monitoring, and risk assessments as part of their cybersecurity audits. Critical national infrastructure operators face similar requirements, as they are considered top-priority sectors for protection. The compliance-driven environment ensures that organizations invest in IDPS solutions not only for security but also to avoid penalties, maintain licenses, and qualify for government contracts.

Key aspects of compliance include centralized logging, intrusion signature management, incident detection within defined timeframes, and mandatory reporting of cyberattacks. Vendors who align their IDPS offerings with these frameworks, and who provide localized compliance mapping, win favor in procurement. For buyers, investing in IDPS becomes an operational requirement rather than a discretionary expense.

In effect, regulatory pressure accelerates the procurement of IDPS solutions, shortens sales cycles for compliant vendors, and ensures long-term integration of IDPS into Saudi organizations' cybersecurity strategies.

More than 70% of Saudi banks report compliance spending as a primary cybersecurity budget driver.

Around 65% of regulated enterprises increased investment in detection systems following new NCA requirements.

Over 80% of government IT contracts include explicit cybersecurity compliance clauses.

Key Market Challenges

Evolving and Sophisticated Threat Landscape:

The first major challenge facing the IDPS market in Saudi Arabia is the rapidly evolving and increasingly sophisticated cyber threat landscape. In recent years, the Kingdom has witnessed a surge in cyberattacks, driven by various factors such as geopolitical tensions, the prevalence of digitalization, and the rising capabilities of cybercriminals. These attacks range from malware and ransomware to distributed denial of service (DDoS) assaults and advanced persistent threats (APTs).

The pace of evolution in cyber threats poses a considerable challenge to the effectiveness of IDPS solutions. Traditional IDPS systems are designed to detect known attack patterns or signatures. However, the landscape is shifting towards zero-day attacks, which are previously unseen and, therefore, lack known signatures. This necessitates more advanced and adaptive solutions, such as anomaly-based detection and machine learning algorithms, which can identify suspicious activities based on deviations from established baselines.

Challenges arise in implementing these advanced IDPS systems effectively. It requires continuous monitoring, threat intelligence sharing, and the fine-tuning of algorithms to ensure accurate detection without an overwhelming number of false positives. The ability to keep pace with rapidly evolving cyber threats, adapt to new attack techniques, and identify unknown threats remains a significant challenge in the Saudi Arabian IDPS market.

Key Market Trends

Integration with Security Orchestration and Automation (SOAR):

The Saudi Arabian IDPS market is the integration of IDPS systems with Security Orchestration, Automation, and Response (SOAR) platforms. SOAR solutions offer the ability to streamline and automate security operations, including incident response, threat detection, and remediation. By combining IDPS with SOAR, organizations can create a more coordinated and efficient security ecosystem.

The Kingdom of Saudi Arabia recognizes the importance of incident response capabilities and is actively strengthening its cybersecurity incident response capabilities. The integration of IDPS with SOAR allows for a more synchronized approach to threat management. When IDPS systems detect an intrusion or potential threat, SOAR

platforms can orchestrate a response, triggering actions such as isolating affected devices, notifying security teams, and gathering additional threat intelligence.

This trend is particularly beneficial for Saudi organizations that deal with large volumes of security alerts and require a systematic way to prioritize and address them. SOAR platforms provide a centralized dashboard for monitoring and responding to security events, enhancing the effectiveness of incident response teams

As the cybersecurity landscape in Saudi Arabia continues to evolve, the integration of IDPS with SOAR reflects the Kingdom's commitment to staying ahead of the curve in threat detection and incident response. This trend contributes to a more proactive and efficient cybersecurity posture, aligning with Saudi Vision 2030's goal of enhancing national security and data protection.

Key Market Players

Cisco Systems Saudi Arabia Limited

Palo Alto Networks Saudi Arabia Limited

IBM Saudi Arabia Limited

Check Point Software Technologies Saudi Arabia Limited

Fortinet Saudi Arabia Limited

McAfee Saudi Arabia Limited

Symantec Saudi Arabia Limited

Trend Micro Saudi Arabia Limited

SonicWall Saudi Arabia Limited

Sophos Saudi Arabia Limited

Report Scope:

In this report, the Saudi Arabia Intrusion Detection and Prevention Systems Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Saudi Arabia Intrusion Detection and Prevention Systems Market, By Components:

Solutions

Services

Saudi Arabia Intrusion Detection and Prevention Systems Market, By Type:

Network-Based

Wireless-based

Network behavior analysis

Host-based

Saudi Arabia Intrusion Detection and Prevention Systems Market, By Industry Verticals:

Banking, Financial Services and Insurance (BFSI)

Government and Defense

Healthcare

Information Technology (IT) and Telecom

Retail and eCommerce

Manufacturing

Others

Saudi Arabia Intrusion Detection and Prevention Systems Market, By Region:

Riyadh

Makkah

Madinah

Jeddah

Tabuk

Eastern Province

Rest of Saudi Arabia

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Saudi Arabia Intrusion Detection and Prevention Systems Market.

Available Customizations:

Saudi Arabia Intrusion Detection and Prevention Systems Market report with the given market data, TechSci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

Contents

1. PRODUCT OVERVIEW

- 1.1. Market Definition
- 1.2. Scope of the Market
 - 1.2.1. Markets Covered
 - 1.2.2. Years Considered for Study
 - 1.2.3. Key Market Segmentations

2. RESEARCH METHODOLOGY

- 2.1. Objective of the Study
- 2.2. Baseline Methodology
- 2.3. Formulation of the Scope
- 2.4. Assumptions and Limitations
- 2.5. Sources of Research
 - 2.5.1. Secondary Research
 - 2.5.2. Primary Research
- 2.6. Approach for the Market Study
 - 2.6.1. The Bottom-Up Approach
 - 2.6.2. The Top-Down Approach
- 2.7. Methodology Followed for Calculation of Market Size & Market Shares
- 2.8. Forecasting Methodology
 - 2.8.1. Data Triangulation & Validation

3. EXECUTIVE SUMMARY

4. VOICE OF CUSTOMER

5. SAUDI ARABIA INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OVERVIEW

6. SAUDI ARABIA INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

- 6.1. Market Size & Forecast
 - 6.1.1. By Value
- 6.2. Market Share & Forecast

6.2.1.By Components (Solutions, Services)

6.2.2.By Type (Network-Based, Wireless-based, Network behavior analysis, Host-based)

6.2.3.By Industry Verticals (Banking, Financial Services and Insurance (BFSI), Government and Defense, Healthcare, Information Technology (IT) and Telecom, Retail and eCommerce, Manufacturing, Others)

6.2.4.By Region (Riyadh, Makkah, Madinah, Jeddah, Tabuk, Eastern Province)

6.3. By Company (2024)

6.3. Market Map

8. RIYADH INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

8.1. Market Size & Forecast

8.1.1.By Value

8.2. Market Share & Forecast

8.2.1.By Components

8.2.2.By Type

8.2.3.By Industry Verticals

9. MAKKAH INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

9.1. Market Size & Forecast

9.1.1.By Value

9.2. Market Share & Forecast

9.2.1.By Components

9.2.2.By Type

9.2.3.By Industry Verticals

10. MAKKAH INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

10.1. Market Size & Forecast

10.1.1. By Value

10.2. Market Share & Forecast

10.2.1. By Components

10.2.2. By Type

10.2.3. By Industry Verticals

11. MADINAH INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

11.1. Market Size & Forecast

11.1.1. By Value

11.2. Market Share & Forecast

11.2.1. By Components

11.2.2. By Type

11.2.3. By Industry Verticals

12. JEDDAH INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

12.1. Market Size & Forecast

12.1.1. By Value

12.2. Market Share & Forecast

12.2.1. By Components

12.2.2. By Type

12.2.3. By Industry Verticals

13. TABUK INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

13.1. Market Size & Forecast

13.1.1. By Value

13.2. Market Share & Forecast

13.2.1. By Components

13.2.2. By Type

13.2.3. By Industry Verticals

14. EASTERN PROVINCE INTRUSION DETECTION AND PREVENTION SYSTEMS MARKET OUTLOOK

14.1. Market Size & Forecast

14.1.1. By Value

14.2. Market Share & Forecast

14.2.1. By Components

14.2.2. By Type

14.2.3. By Industry Verticals

15. MARKET DYNAMICS

15.1. Drivers

15.2. Challenges

16. MARKET TRENDS AND DEVELOPMENTS

17. COMPANY PROFILES

17.1. Cisco Systems Saudi Arabia Limited

17.1.1. Business Overview

17.1.2. Key Revenue and Financials

17.1.3. Recent Developments

17.1.4. Key Personnel/Key Contact Person

17.1.5. Key Product/Services Offered

17.2. Palo Alto Networks Saudi Arabia Limited

17.2.1. Business Overview

17.2.2. Key Revenue and Financials

17.2.3. Recent Developments

17.2.4. Key Personnel/Key Contact Person

17.2.5. Key Product/Services Offered

17.3. IBM Saudi Arabia Limited

17.3.1. Business Overview

17.3.2. Key Revenue and Financials

17.3.3. Recent Developments

17.3.4. Key Personnel/Key Contact Person

17.3.5. Key Product/Services Offered

17.4. Check Point Software Technologies Saudi Arabia Limited

17.4.1. Business Overview

17.4.2. Key Revenue and Financials

17.4.3. Recent Developments

17.4.4. Key Personnel/Key Contact Person

17.4.5. Key Product/Services Offered

17.5. Fortinet Saudi Arabia Limited

17.5.1. Business Overview

17.5.2. Key Revenue and Financials

17.5.3. Recent Developments

- 17.5.4. Key Personnel/Key Contact Person
- 17.5.5. Key Product/Services Offered
- 17.6. McAfee Saudi Arabia Limited
 - 17.6.1. Business Overview
 - 17.6.2. Key Revenue and Financials
 - 17.6.3. Recent Developments
 - 17.6.4. Key Personnel/Key Contact Person
 - 17.6.5. Key Product/Services Offered
- 17.7. Symantec Saudi Arabia Limited
 - 17.7.1. Business Overview
 - 17.7.2. Key Revenue and Financials
 - 17.7.3. Recent Developments
 - 17.7.4. Key Personnel/Key Contact Person
 - 17.7.5. Key Product/Services Offered
- 17.8. Trend Micro Saudi Arabia Limited
 - 17.8.1. Business Overview
 - 17.8.2. Key Revenue and Financials
 - 17.8.3. Recent Developments
 - 17.8.4. Key Personnel/Key Contact Person
 - 17.8.5. Key Product/Services Offered
- 17.9. SonicWall Saudi Arabia Limited
 - 17.9.1. Business Overview
 - 17.9.2. Key Revenue and Financials
 - 17.9.3. Recent Developments
 - 17.9.4. Key Personnel/Key Contact Person
 - 17.9.5. Key Product/Services Offered
- 17.10. Sophos Saudi Arabia Limited
 - 17.10.1. Business Overview
 - 17.10.2. Key Revenue and Financials
 - 17.10.3. Recent Developments
 - 17.10.4. Key Personnel/Key Contact Person
 - 17.10.5. Key Product/Services Offered

18. STRATEGIC RECOMMENDATIONS

19. ABOUT US & DISCLAIMER

I would like to order

Product name: Saudi Arabia Intrusion Detection and Prevention Systems Market By Components (Solutions, Services), By Type (Network-Based, Wireless-based, Network behavior analysis, Host-based), By Industry Verticals (Banking, Financial Services and Insurance (BFSI), Government and Defense, Healthcare, Information Technology (IT) and Telecom, Retail and eCommerce, Manufacturing, Others) By Region, Competition, Forecast & Opportunities, 2020-2030F

Product link: <https://marketpublishers.com/r/S058AAF42448EN.html>

Price: US\$ 3,500.00 (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/S058AAF42448EN.html>