+44 20 8123 2220
info@marketpublishers.com

Saudi Arabia Operational Technology Security Market, Segmented By Offering (Solution, Services), By Organization Size (Small and Medium Organization, and Large Organization), By Deployment Mode (On-Premises and Cloud), By End User (Manufacturing, BFSI, Energy & Power, Logistics & Supply Chain, Mining, Oil & Gas, and Others), By Region, Competition, Forecast and Opportunities, 2028

https://marketpublishers.com/r/S1A4FDE0BC9BEN.html
Date: October 2023
Pages: 88
Price: US$ 3,500.00 (Single User License)
ID: S1A4FDE0BC9BEN

Abstracts

The market for operation technology (OT) security in Saudi Arabia is expected to grow in the coming years. OT security refers to the protection of physical devices and systems that are used in industrial and infrastructure sectors such as oil and gas, power and water utilities, transportation, and manufacturing. These systems are critical to the functioning of various industries and are increasingly being connected to the internet, making them vulnerable to cyber-attacks. Saudi Arabia is one of the largest producers of oil and gas in the world and has a significant presence in other industries such as power and water utilities, transportation, and manufacturing. As these industries continue to modernize and digitize their operations, the need for OT security solutions has become increasingly important. The Middle East and Africa region, which includes Saudi Arabia, is expected to be one of the fastest-growing markets for OT security during this period. Several factors are driving the demand for OT security solutions in Saudi Arabia, including the increasing adoption of internet-connected devices and systems, rising awareness about the risks of cyber-attacks, and the growing need to comply with regulatory requirements. The Saudi Arabian government has also recognized the importance of OT security and has taken several measures to enhance the cybersecurity posture of critical infrastructure sectors. Overall, the market for OT

+44 20 8123 2220
info@marketpublishers.com

security in Saudi Arabia is expected to grow in the coming years, driven by increasing demand from various industries and government initiatives to improve cybersecurity.

The future of operational technology (OT) security is expected to be shaped by several trends and developments in the field of cybersecurity and industrial automation. With the increasing use of digital technologies and the Internet of Things (IoT) in industrial systems, the boundaries between IT and OT security are blurring. As a result, organizations are likely to adopt a converged approach to cybersecurity, where IT and OT security are integrated into a single framework. Machine learning and AI technologies are increasingly being used in cybersecurity to detect and respond to cyber threats in real-time. In the future, we can expect to see more adoption of these technologies in OT security to enhance the detection and response capabilities of organizations. As industrial systems become more interconnected, the supply chain is becoming a critical area of concern for OT security. Organizations need to focus on securing their supply chain and ensuring that their vendors and suppliers are following best practices in cybersecurity. Many organizations are struggling to keep up with the rapidly evolving threat landscape in OT security. As a result, there is a growing demand for managed OT security services, where third-party providers offer end-to-end security solutions and services to organizations. There is a need for new standards and frameworks that address the unique challenges of OT security.

Overall, the future of OT security is likely to be shaped by the convergence of IT and OT security, the adoption of machine learning and AI, increased focus on supply chain security, growing demand for managed OT security services, and development of new OT security standards and frameworks.

The Increased Use of Digital Technologies in Industrial Systems

The increased use of digital technologies in industrial systems is another major driver of the market growth of operational technology (OT) security in Saudi Arabia. Digital technologies such as cloud computing, big data analytics, and the Internet of Things (IoT) are transforming the way industries operate and manage their assets, leading to improved efficiency, productivity, and cost savings. However, with the increased adoption of digital technologies in industrial systems, the risk of cyber-attacks has also increased significantly. Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems that are used in critical infrastructure sectors such as oil and gas, power and water utilities, transportation, and manufacturing are often vulnerable to cyber-attacks, which can result in operational downtime, physical damage,

and even loss of life. As a result, there is a growing need for OT security solutions in Saudi Arabia to protect these critical industrial systems from cyber threats. OT security solutions such as firewalls, intrusion detection systems, and security information and event management (SIEM) systems are becoming more widely adopted by organizations to protect their ICS and SCADA systems from cyber-attacks. The Saudi Arabian government has also recognized the importance of OT security and has taken several measures to enhance the cybersecurity posture of critical infrastructure sectors. For example, the National Cybersecurity Authority (NCA) has launched various initiatives to raise awareness about the importance of cybersecurity in critical infrastructure sectors and has provided guidelines and frameworks for organizations to improve their OT security measures. Overall, the increased use of digital technologies in industrial systems is a key driver of the market growth of OT security in Saudi Arabia, as organizations seek to protect their critical infrastructure from cyber threats and comply with regulatory requirements.

Increase in adoption of Industrial Internet of Things (IIoT) Solutions

The increase in adoption of industrial internet of things (IIoT) solutions is another major driver of the market growth of operational technology (OT) security in Saudi Arabia. IIoT refers to the use of internet-connected devices and sensors in industrial systems to collect and analyze data, leading to improved efficiency, productivity, and cost savings. However, with the increased adoption of IIoT solutions in industrial systems, the risk of cyber-attacks has also increased significantly. IIoT devices and sensors that are used in critical infrastructure sectors such as oil and gas, power and water utilities, transportation, and manufacturing are often vulnerable to cyber-attacks, which can result in operational downtime, physical damage, and even loss of life. As a result, there is a growing need for OT security solutions in Saudi Arabia to protect these critical industrial systems from cyber threats. OT security solutions such as firewalls, intrusion detection systems, and network segmentation are becoming more widely adopted by organizations to protect their IIoT devices and sensors from cyber-attacks. The Saudi Arabian government has also recognized the importance of OT security and has taken several measures to enhance the cybersecurity posture of critical infrastructure sectors. For example, the National Cybersecurity Authority (NCA) has launched various initiatives to raise awareness about the importance of cybersecurity in critical infrastructure sectors and has provided guidelines and frameworks for organizations to improve their OT security measures. Overall, the increase in adoption of IIoT solutions is a key driver of the market growth of OT security in Saudi Arabia, as organizations seek to protect their critical infrastructure from cyber threats and comply with regulatory requirements.

+44 20 8123 2220
info@marketpublishers.com

Rising Digitalization among Enterprises is Driving the Market Growth.

Rising digitalization among enterprises is indeed driving the market growth of operational technology security in Saudi Arabia. As more and more businesses embrace digital transformation, the demand for operational technology security such as software development, cybersecurity, cloud computing, and data analytics has increased significantly. Furthermore, the COVID-19 pandemic has accelerated the pace of digitalization across businesses, as remote work and online transactions have become the new normal. This has further boosted the demand for operational technology security, as companies need to ensure the security and efficiency of their digital infrastructure. Overall, the market for operational technology security in Saudi Arabia is expected to continue its growth trajectory, driven by the increasing adoption of digital technologies and the growing demand for innovative solutions. Overall, the rising digitalization among enterprises is driving the growth of the operational technology security market, and this trend is expected to continue in the coming years.

Market Segmentation

The Saudi Arabia operational technology security market is segmented into offering, organization size, deployment mode, end user, and region. Based on offering, the market is segmented into solution and services. Based on organization size, the market is segmented into small and medium organization and large organization. Based on deployment mode, the market is segmented into on-premises and cloud. Based on end user, the market is further split into manufacturing, BFSI, energy & power, logistics & supply chain, mining, oil & gas, and others. The market analysis also studies the regional segmentation to devise regional market segmentation, divided among Northern & Central Region, Eastern Region, Southern Region, and Western Region.

Company Profiles

Some of the major players in the operational technology security market include Honeywell International Inc., Cisco Systems, Inc., CyberArk software Ltd., Kaspersky Lab, Fortinet, Inc., Microsoft Corporation, Forcepoint LLC, Palo Alto Networks, Nozomi Networks, and T?V S?D AG. Major companies operating in the market are following strategies such as mergers & acquisitions, new products & services launches, among others, to stay competitive in the market and have an edge over the competitors.

Report Scope:

+44 20 8123 2220
info@marketpublishers.com

In this report, the Saudi Arabia operational technology security market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Saudi Arabia Operational Technology Security Market, By Service:

Solution

Services

Saudi Arabia Operational Technology Security Market, By Organization Size:

Large Enterprises

Small & Medium-sized Enterprises

Saudi Arabia Operational Technology Security Market, By Deployment Mode:

On-Premises

Cloud

Saudi Arabia Operational Technology Security Market, By End User:

Manufacturing

BFSI

Energy & Power

Logistics & Supply Chain

Mining

Oil & Gas

Others

+44 20 8123 2220
info@marketpublishers.com

Saudi Arabia Operational Technology Security Market, By Region:

Northern & Central Region

Eastern Region

Southern Region

Western Region

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Saudi Arabia operational technology security market.

Available Customizations:

With the given market data, Tech Sci 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).

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

(Note: The companies list can be customized based on the client requirements.)

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Saudi Arabia Operational Technology Security Market, Segmented By Offering (Solution, Services), By Organization Size (Small and Medium Organization, and Large Organization), By Deployment Mode (On-Premises and Cloud), By End User (Manufacturing, BFSI, Energy & Power, Logistics & Supply Chain, Mining, Oil & Gas, and Others), By Region, Competition, Forecast and Opportunities, 2028

Product link: https://marketpublishers.com/r/S1A4FDE0BC9BEN.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/S1A4FDE0BC9BEN.html

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:
Last name:
Email:
Company:
Address:
City:
Zip code:
Country:
Tel:
Fax:
Your message:

**All fields are required

Custumer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at https://marketpublishers.com/docs/terms.html

+44 20 8123 2220
info@marketpublishers.com

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970