Middle East Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

https://marketpublishers.com/r/MA97FB214E5AEN.html

Date: July 2024
Pages: 142
Price: US$ 4,750.00 (Single User License)
ID: MA97FB214E5AEN

Abstracts

The Middle East Cybersecurity Market size is estimated at USD 10.81 billion in 2024, and is expected to reach USD 15.96 billion by 2029, growing at a CAGR of 8.10% during the forecast period (2024-2029).

The key drivers contributing to the increase in the adoption of data-intensive approaches and decisions with the growth include the increase in the number of cyberattacks in the Middle East with the growing digitalization.

Key Highlights

The pandemic boosted digital transformation in the Middle East and increased the demand for cybersecurity solutions to protect remote work environments. Businesses prioritize robust cyber defenses, fueling growth in the cybersecurity market across the region.

Earlier, the Middle East did not witness a significant target for cyberattacks. Regions such as Europe and North America have always been majorly affected by cyber threats. However, rapid digitalization in countries such as Saudi Arabia and the UAE has recently boosted the number of connected devices, opening new gateways for cyberattacks.

Governments in the region are also growing their investments in information and communication technology. As a result, the region's social infrastructure, financial sector, government services, schools, and hospitals have been deploying interconnectivity solutions with less attention to these developments' security

requirements.

However, the significant factors driving the threat of cyberattacks in the Middle East are increasing vulnerabilities in digital communications networks and supply chains, rapid development in the user base of online consumers, and, chiefly, the deficient cybersecurity infrastructure.

Traditional authentication methods, such as passwords, PINs, and security tokens, have been the cornerstone of digital security for many years. Users must remember and provide unique credentials to access their accounts or sensitive data. While these methods are popular, they also have drawbacks, such as weak passwords, reused passwords, and vulnerability to phishing attacks. The high reliance on these traditional authentication methods is posing a challenge to the market's growth.

As the economy moves toward digital transformation aligned with Saudi Vision 2030, more businesses are adopting cloud solutions and other online application platforms. In addition, the number of accessible components remotely is also rising across industries, providing additional points of vulnerability. These factors contribute to the increased cyber-attack rate, driving the demand for effective cybersecurity measures in the post-COVID-19 Scenario.

Middle East Cybersecurity Market Trends

Cloud to Witness Significant Growth

Numerous factors, including scalability, flexibility, ease of accessibility, and cost-effectiveness, drive the growing adoption of cloud-based cybersecurity solutions. The increasing reliance on remote and mobile capabilities contributes to the demand for cloud-based cybersecurity. Cloud solutions can facilitate secure access and monitoring of systems from any location, supporting the needs of modern, flexible work environments.

Deploying cloud-based services can significantly reduce the Capex requirement as the companies need not invest in hardware components. Cloud solutions also enable better prediction of the cost of an application, and companies do not need to incur much upfront cost to incorporate the technology. The hardware and IT support savings make cloud-based solutions much more affordable.

The growing collaborative efforts of cloud solution providers are driving cloud adoption

in the public and private sectors in the country and developing the cloud environment. This growth in adopting cloud solutions creates a need for cloud-based cybersecurity solutions. Saudi Arabia is anticipated to drive the demand for cloud-based cybersecurity solutions due to the rapid adoption of cloud technology and growing investment in digital transformation. As organizations increasingly rely on cloud-based services and data storage, the need for this solution is rising in the country. In addition, companies such as Oracle Corp plan to boost their cloud offerings in Saudi Arabia and the UAE with more cloud regions.

Overall, the growth of cloud-based solutions is driven by its ability to address the evolving needs of organizations in an increasingly digital and interconnected environment. Cloud-based cybersecurity solutions are expected to gain prominence as organizations encounter the complexities of a dynamic threat landscape and undergo digital transformations.

The surge in 5G subscribers across the Middle East is catalyzing digital transformation by delivering heightened connectivity and accelerated data transfer speeds. This technological development empowers businesses to adopt advanced applications and innovative solutions. However, the expanded digital landscape also exposes businesses to heightened cybersecurity threats. As reliance on 5G infrastructure grows, so does the imperative for robust cybersecurity measures to safeguard against potential vulnerabilities and cyberattacks.

The demand for cybersecurity solutions in the Middle East region is escalating, driven by the need to fortify networks, protect sensitive information, and ensure the resilience of critical digital assets in the face of evolving cyber threats. According to Ericsson, 5G subscriptions in the GCC are expected to reach 74.59 million by 2029. In 2023, there were 25.74 million 5G subscriptions in the GCC.

United Arab Emirates (UAE) to Witness Major Growth

The Middle East region has one of the most sensitive areas of cyberspace in the world. The combination of high digitization rates and a thriving economy is drawing the attention of malicious actors' attention worldwide. According to Microsoft, from July 2022 to June 2023, nearly 38% of the network interruptions in the Middle Eastern nations by nation-state or state-affiliated cyber threat performers were absorbed against Israel. The UAE ranked second in the part of threats in the region.

The UAE is one of the prominent economies. It has focused on moving toward a digital economy for the last few years, combined with government initiatives and increased interest from global and local vendors. In addition, government initiatives such as the "Cyber Sniper" to sharpen the skills of national talents, raise awareness on cybersecurity issues, enhance the cybersecurity capabilities of specialized government personnel, and enrich the experiences of professionals in federal entities are expected to impact the cybersecurity landscape in the region positively.

Further, with the emphasis on digitalization, its vulnerabilities are also growing, driving the demand for cybersecurity solutions and services in the country. For instance, according to the head of the UAE's Cybersecurity Council, over 71 million attempted cyberattacks in the UAE have been blocked in the first three quarters of 2023.

The growing pace of technology adoption in the UAE, including remote work tools and migration to the cloud, has bolstered the demand for cybersecurity solutions and services in the country's businesses. Global market vendors are capitalizing on the opportunity and expanding their regional cybersecurity service offerings by partnering with local companies.

Overall, the cybersecurity market in the country is analyzed to witness substantial growth largely due to growing technology adoption, partnerships among market vendors and end-users, government initiatives in the cybersecurity landscape, and the growing presence of global market vendors offering their cybersecurity services in the region.

Middle East Cybersecurity Industry Overview

The Middle Eastern cybersecurity market is fragmented, consisting of established tech giants and new competitors. Some players include IBM Corporation, Fortinet Inc., Cisco Systems Inc., Trend Micro Inc., and Microsoft Corporation.

January 2024 - Middlesex University (MDX) Dubai partnered with Fortinet by joining its Academic Partner Programme. The partnership offers a significant initiative forward in the university's commitment to elevating cybersecurity education in the UAE. As an Academic Partner, MDX Dubai will integrate Fortinet NSE certifications directly into its existing courses and facilitate the content as standalone self-paced learning for students. It also supports the UAE Cybersecurity Council, which has set out to develop

a comprehensive cybersecurity strategy and a safe and strong cyberinfrastructure in the region.

November 2023 - Trend Micro signed a Memorandum of Understanding (MoU) with Zero&One, the MENA region's pioneering Premier AWS partner with DevOps, Application Modernization, AWS Migration and Cost Optimization expertise. The partnership represents a collaborative endeavor to reshape and elevate the digital landscape through robust, advanced cloud security solutions meticulously tailored to address the region's requirements and challenges.

Additional Benefits:

The market estimate (ME) sheet in Excel format

3 months of analyst support

Contents

8 FUTURE OUTLOOK OF THE MARKET

I would like to order

Product name: Middle East Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

Product link: https://marketpublishers.com/r/MA97FB214E5AEN.html

Price: US$ 4,750.00 (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/MA97FB214E5AEN.html