+357 96 030922
info@marketpublishers.com

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

https://marketpublishers.com/r/MC2C5F91C065EN.html
Date: July 2024
Pages: 100
Price: US$ 4,750.00 (Single User License)
ID: MC2C5F91C065EN

Abstracts

The MEA Cybersecurity Market size is estimated at USD 2.91 billion in 2024, and is expected to reach USD 5.23 billion by 2029, growing at a CAGR of 12.42% during the forecast period (2024-2029).

Key Highlights

In the current market scenario, Cybersecurity clusters can grow organically or develop through intentional, often top-down actions taken by local governments, and government regulations and policies play a significant role in their development. Many private firms have been moving their operations to the cloud platform.

Saudi Arabia, an oil-based economy, is the largest in the Gulf region and aims to be the most prominent IT market. Like the National Transformation Program (NTP), several government initiatives have supported the region's rapid IT development. Saudi Arabia is a popular target for cybercriminals due to its oil wells and occupancy of an area prevalent with geopolitical tensions. Under the NTP initiative, the government outlined SAR 4 billion for ICT development from 2016 until the previous year. The main focus areas are cybersecurity, smart grid, and geospatial IT systems to control significant infrastructure. Such a push from the government provides scope for IT security companies to flourish within the country.

According to Help AG's State of the Market Report of the previous year, there was a 183% rise in attacks in the UAE alone. All sectors in the nation faced repeated attacks, including the government, oil, healthcare, and telecom. Distributed Denial of Service (ddos) has only increased in scale, according to the company, with the UAE measuring 254.3 Gbps. Further, the growth in the number of smes and cybersecurity vendors in

+357 96 030922
info@marketpublishers.com

the country is directing focus on offering innovative solutions. Thus, vendors are expected to adopt new launches as part of their competitive strategy. For example, UAE-based Coordinates announced Adaptive Bespoke Cybersecurity for SME.

To support Qatar's efforts to address the current and emerging threats and risks, and in light of the strategic thrusts of Qatar's National ICT Plan to protect the national critical information infrastructure providing a safe and secure online environment for the different sectors, Qatar National Cyber Security Strategy (NCSS) was created by the National Cyber Security Committee (NCSC). The NCSC was primarily established under the Prime Minister's Decision No. (18) to provide a governance structure for collaboratively addressing cyber security at the highest levels of the government.

The Middle East & Africa region have smaller numbers of cybersecurity workforces. Still, considering the region's high degree of business activities, it is one of the most attractive regions for cyber attacks. Also, most professionals in this region need to be more experienced in dealing with the intensity of incoming cyber threats. For instance, According to Fircroft, around 30% of all cybersecurity workforce in the Middle East have just over ten years of experience working in the industry. In comparison, 60% of these professionals have more than five years of experience.

Enterprises adopting remote working during the covid-19 increased the number of attacks. According to IBM, the average cost was USD 1.05 million higher in breaches where remote work was a factor in causing the breach compared to those where remote work was not a factor. According to a study by Proofpoint in 2021 (N=1,400 respondents; Chief Information Security Officers (cisos) from organizations with more than 200 employees), about 76% CISO's from UAE and 69% of CISO's from KSA part of the study mentioned their business had seen more targeted attacks since enabling widespread remote working worldwide in 2021.

Middle East & Africa Cybersecurity Market Trends

Cloud Segment is expected to grow at a higher pace.

The increasing use of cloud-based managed security services has even simplified the adoption of cybersecurity practices for Middle Eastern enterprises. Cloud security refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from threats. Cloud security stands out from the legacy as a modernized cyber security solution. IT models include scaling speeds, data storage, end-user system interfacing, and proximity to other networked data and systems.

+357 96 030922
info@marketpublishers.com

Cloud computing has transformed how enterprises use, share, and store data, applications, and workloads. However, it has also introduced a host of new security threats and challenges. Significant data going into the cloud and public cloud services increases the exposure. The cloud market in UAE is still in the early stages, with the implementation of private laaS viewed as a critical first step towards broader cloud adoption. The opening of cloud data centers in the region is likely to boost cloud adoption, which would drive the demand for cloud security. Also, initiatives by the countries in the region to move towards a cloud computing future are poised to propel the demand for cloud security.

To tap the market opportunities, vendors in MEA need to innovate cloud-based solutions. They also want to build global data centers to strengthen cloud resilience, meet data privacy regulations, and engage with the public cloud (AWS, Azure) for higher scalability.For instance, Bahrain Economic Development Board (EDB) signed a Memorandum of Understanding (MoU) with Tencent Cloud, the cloud computing subsidiary of the multinational Chinese tech firm, to drive the Kingdom of Bahrain's IDC development and support its rapid emergence as the MENA region's hub for the cloud and IDC sectors by opening an Internet Data Centre (IDC) in the country. Establishing such public cloud infrastructures is expected to drive the demand for cloud-based solutions in the MENA region.

However, Africa still needs to catch up to the deployment of cloud solutions as compared to the Middle Eastern region. Piracy is still a big hurdle as many businesses use legacy on-prem versions of pirated software. However, this exposes the company to multiple threats. With security threats across the region increasing in frequency and sophistication, vendors in the area are offering Cloud UTM that provides organizations with around-the-clock protection and the cloud's scalability. It eliminates the complexity of managing on-premise firewalls and delivers superior identification and threat management. For instance, recently, du, from Emirates Integrated Telecommunications Company (EITC), has launched its Cloud Unified Threat Management (UTM) service, a cybersecurity solution that extends organizations' perimeters to all sites securely.

According to Turbonomic, in 2021, 56 % of respondents said they use Microsoft Azure for cloud services. Amazon Web Services (AWS) topped the ranking until 2020 when Microsoft surpassed it. Furthermore, the percentage of respondents who do not use any cloud increased from 4% in 2021 to 8% in the last year.

+357 96 030922
info@marketpublishers.com

BFSI is Expected to Drive the Market

The Middle Eastern and African region is undergoing digital transformations from a broader economic development context and within the banking sector. Before COVID-19, BFSI digitalization rates in the area were low; however, as the threat and uncertainty from COVID-19 settled in, the financial services industry is started adopting digitization at a rapid pace and utilizing technologies such as cloud, artificial intelligence (AI), to meet rising customer expectations to remain competitive.

The UAE Banks Federation (UBF), a professional body representing 49 banks as members in 2021, announced that it is launching a new initiative to combat all future cyber threats. As a part of this initiative, all the member banks will have to seamlessly collect, analyze and share data on cyber threats while allowing anonymous reporting and alert management. The initiative will enable financial institutions to gain an encompassing perceptive of the ongoing cyber threat landscape. It will allow them to better prepare and respond to all emergent threats.

The National Bank of Fujairah (NBF) has built a robust cybersecurity strategy focusing on three main pillars: identity protection, data protection, and culture. Moreover, as part of the bank's cyber resiliency program, it conducts various types of cyberattack simulations like the Red Team exercise, Tabletop Cyber Attack Simulations, and Phishing simulations, among others, to measure our cyber resiliency capabilities with the help of specialists.

According to AFDB, this ACRC project has the potential to benefit over 250 million vulnerable clients and over 2,000 financial institutions across the region. Moreover, as part of its gender promotion policy, ACRC will specifically target improving cybersecurity for 20 to 25 million women in five years and will aim to employ a workforce of at least 39% of women. Investments in the awareness of cybercrime in the BFSI sector in the region are expected to drive the development of solutions offered during the forecasted period.

According to Milken Institute, in the Middle East area, the number of financial technology (FinTech) enterprises is predicted to grow to 465 by 2022. There were just 30 fintech companies in the region in 2017. The gradual growth of fintech firms in the region creates an opportunity for the local and international players to develop new solutions to capture the market share.

+357 96 030922
info@marketpublishers.com

Middle East & Africa Cybersecurity Industry Overview

The cybersecurity market in the Middle East and Africa is highly competitive and consists of several major players. In terms of market share, few of the major players currently dominate the market. These major players with a prominent market share are focusing on expanding their customer bases across foreign countries. These companies leverage strategic collaborative initiatives to increase their market shares and profitability.

In March 2023, the International Civil Aviation Organization announced new developments and progress in areas of aviation cybersecurity and innovation with the UAE Government. The ICAO-UAE partnership is expected to enhance knowledge sharing and experience in terms of cybersecurity, accelerators, and innovation in future civil aviation.

Additional Benefits:

The market estimate (ME) sheet in Excel format

3 months of analyst support

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

6 COMPETITIVE LANDSCAPE

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

I would like to order

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

Product link: https://marketpublishers.com/r/MC2C5F91C065EN.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/MC2C5F91C065EN.html