Qatar Cybersecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 100 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:

The Qatari cybersecurity market is expected to register a CAGR of 12.6% during the forecast period.

Key Highlights
Organizations are fighting on all fronts to combat the rising cyber dangers as the world moves toward a more digital landscape. Currently, enterprises have to traverse a more complicated threat landscape due to the recent changes. The challenges of safeguarding digital activities with the hybrid work model have also prompted enterprises to reassess their security approach with robust, industry-leading security solutions.
Qatar has been at the forefront of preventing the spread of cyber-attacks and creating a safe environment. The country has developed an advanced cyber security platform, Warning, to identify and detect security threats against corporations and infrastructure systems. The platform is the result of a three-year collaboration between the QCRI, the Ministry of Interior, the Supreme Committee for Delivery and Legacy, TOBB University of Economics and Technology in Turkey, Kadir Has University, and Interprobe, a cyber-defense firm.
The widespread adoption of hybrid work environments and the increased usage of digital-centric communication channels have expanded the attack surface, creating new organizational security risks for people and data. By safeguarding email and business communications, the Mimecast X1 Platform is engineered to leverage a rich intelligence source to learn about people and how they collaborate. These insights enable organizations to work safely by protecting their people, data, and communications.
The organization of massive sports events, such as Formula One, and Fifa World Cup, attracts cyber attacks on networks and the country's critical infrastructure. With such events being conducted in the country, the government has initiated various projects to improve the country's cybersecurity.
Due to the COVID-19 outbreak, the country implemented preventive measures such as lockdowns, leading to the shutting down of offices and increasing the trend of work-from-home. The increase in remote connections, augmented by work-from-home and the

adoption of BYOD, increases the scope of cyber threats in the region, thus resulting in the rising adoption of various cybersecurity solutions.

Qatar Cybersecurity Market Trends

Rapidly Increasing Cybersecurity Incidents Driving the Market

The global penetration of the internet and the adoption of payment-linked online services, which attract profit-seeking criminals, are the primary drivers for cyber attacks. Significant reductions in device costs, coupled with emerging business models, have been instrumental in increasing the market penetration of IoT, thus boosting the number of connected devices, such as connected cars, machines, meters, wearables, and consumer electronics.
Cybersecurity incidents in the country are continuously increasing as enterprises aggressively embrace digitalization and connected technologies as part of business operations. Qatar's rapidly developing economy depends on various information and communications technology (ICT) platforms for innovation and growth.
Increased ICT use and broadband connectivity bring enormous benefits to the government, businesses, institutions, and individuals. This factor further increases cyber threats, leading to increased adoption of cyber security solutions.
For instance, Trend Micron announced that the company identified and blocked more than 15 million cyber threats in Qatar. Such instances increase the adoption of cybersecurity solutions, thus leading to the growth of the market.

Cloud-deployed Cybersecurity Solutions are Expected to Hold Significant Market Share

The increasing adoption of strategies and technologies for reducing operational costs by using the cloud for data storage is boosting the demand for cloud-based solutions and the adoption of on-demand security services.
Large businesses and SMEs in the region are rapidly switching to cloud-based solutions due to several advantages. Due to the limited financial resources for cybersecurity, SMEs have embraced cloud deployment of cybersecurity solutions as it allows businesses to invest in their core skills rather than allocate significant resources to security infrastructure.
With the increased adoption of cloud services, such as Google Cloud, AWS, and Microsoft Azure, and with these tools emerging as an integral part of business processes, enterprises have to deal with security issues, such as loss of control over sensitive data, thus increasing the incorporation of on-demand cybersecurity solutions.
The rising adoption of cloud-based email security services is encouraging the use of services integrated with other cybersecurity platforms, such as IPS and NGFW. Due to this trend, businesses are becoming less inclined to invest in specialized, on-premise security solutions, thus increasing the demand for cloud-deployed cybersecurity solutions.

Qatar Cybersecurity Market Competitor Analysis

The Qatari cybersecurity market appears to be moderately concentrated, with players adopting key strategies like mergers, acquisitions, and service innovation. Some of the major players in the market are Cisco Systems Inc., MEEZA, Atos SE, Protiviti Inc., IBM Corporation, etc. Some of the recent developments are:

October 2022 - Morocco and Qatar entered a joint cooperation agreement to increase security cooperation and exchange information for the 2022 FIFA World Cup. The agreement also includes increased security in the competition and extends to

general cooperation in the field.
June 2022 - Mandiant Inc. announced the launch of the Mandiant Cyber Alliance Program across the sectors, which include endpoint, network, identity and authentication, security information and event management, and cloud security.

Additional Benefits:

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

Table of Contents:

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

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHTS
4.1 Market Overview
4.2 Value Chain Analysis
4.3 Industry Attractiveness - Porter's Five Forces Analysis
4.3.1 Threat of New Entrants
4.3.2 Bargaining Power of Buyers
4.3.3 Bargaining Power of Suppliers
4.3.4 Threat of Substitutes
4.3.5 Intensity of Competitive Rivalry
4.4 Impact of COVID-19 on the Market

5 MARKET DYNAMICS
5.1 Market Drivers
5.1.1 Rapidly Increasing Cybersecurity Incidents
5.1.2 Increasing Demand for Digitalization and Scalable IT Infrastructure
5.2 Market Restraints
5.2.1 Lack of Cybersecurity Professionals
5.2.2 High Reliance on Traditional Authentication Methods and Low Preparedness
5.3 Trends Analysis
5.3.1 Rising Trends for IoT, BYOD, Artificial Intelligence, and Machine Learning in Cybersecurity
5.3.2 Exponential Growth to be Witnessed in Cloud Security Due to a Shift Toward Cloud-based Delivery Models

6 MARKET SEGMENTATION
6.1 By Offering
6.1.1 Security Type
6.1.1.1 Cloud Security
6.1.1.2 Data Security
6.1.1.3 Identity Access Management

6.1.1.4 Network Security
6.1.1.5 Consumer Security
6.1.1.6 Infrastructure Protection
6.1.1.7 Other Types
6.1.2 Services
6.2 By Deployment
6.2.1 Cloud
6.2.2 On-premise
6.3 By End User
6.3.1 BFSI
6.3.2 Healthcare
6.3.3 Manufacturing
6.3.4 Government and Defense
6.3.5 IT and Telecommunication
6.3.6 Other End Users

7 COMPETITIVE LANDSCAPE
7.1 Company Profiles
7.1.1 IBM Corporation
7.1.2 Cisco Systems Inc.
7.1.3 MEEZA
7.1.4 Broadcom Limited
7.1.5 Dell Technologies Inc.
7.1.6 Atos SE
7.1.7 Protiviti Inc.
7.1.8 Mcafee LLC
7.1.9 Intel Security (Intel Corporation)

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

Qatar Cybersecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 100 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	2025-05-04
		Signature	