

## **UAE Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029**

Market Report | 2024-02-17 | 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 UAE Cybersecurity Market size is estimated at USD 0.59 billion in 2024, and is expected to reach USD 1.07 billion by 2029, growing at a CAGR of 12.72% during the forecast period (2024-2029).

The rapid digitalization in the United Arab Emirates has triggered the number of connected devices by opening new cyberattack gateways. Cybersecurity has become increasingly imperative for governments and companies as digitization has increased due to the COVID-19 pandemic, with digital criminal activity increasing.

#### **Key Highlights**

- A considerable increase in cyberattacks during the COVID-19 pandemic, terrorism threats, and digital transformation have pushed the UAE to secure its cyber borders through high expenditure within its new budget. In October last year, the UAE announced adopting cybersecurity standards for government agencies as the country revealed the budget for the next five years.
- The United Arab Emirates has witnessed a more than 250 percent increase in cyberattacks during the pandemic, according to the UAE Government cybersecurity chief. Ransomware and phishing were the most common forms of attack, and the financial and healthcare sectors were among the most prominent targets. This sudden increase was also attributed to the activists against the UAE's recognition of Israel and normalizing these countries' relationships.
- UAE's government has been emphasizing cybersecurity owing to increasing cyberattacks. For instance, according to the World Economic Forum's (WEF) 'The Global Risks Report' of this year, the risk of cybersecurity failure is ranked among the top five concerns for the UAE.
- As organizations in the UAE undergo digital transformation and move their operations online, the attack surface for cyber threats expands. This provides cybercriminals with more opportunities to target sensitive data and systems.
- Budget constraints and the high cost of cybersecurity solutions can pose challenges for the market, as they can limit the ability of

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

organizations and government entities to protect their digital assets effectively.

-The COVID-19 pandemic created an environment suitable for cyberattacks. Cybercriminals saw new opportunities with a shift to remote work and increased reliance on digital technologies. There was a surge in phishing attacks, malware, and ransomware campaigns targeting individuals and organizations in the UAE.

## UAE Cybersecurity Market Trends

### Stringent Government Regulations for Increasing Adoption of Cybersecurity Solutions is Expected to Drive the Market Growth

- UAE is one of the prominent economies in the Middle East region and has been focusing on moving toward a digital economy for the last few years, combined with government initiatives and increased interest from global and local vendors. Similarly, the country is making headways in digitizing almost every industry in the country. With the emphasis on digitalization, the vulnerabilities associated with it are seeing growth as well.
- Investment drives the demand for ICT products and services in aviation, healthcare, hospitality, retail, and other sectors linked to the UAE's economic diversification plans, such as real estate and manufacturing. UAE ICT market challenges include the high cost of internet access and bandwidth and its exposure to cybersecurity threats. To attract foreign companies and develop human capital resources, the UAE government has established the UAE ICT Fund, which educates hundreds of Emirati students overseas in the ICT field.
- Moreover, the UAE's SmartPass system has created a digital framework for the operations of all government services and ministries. The UAE 2031 AI Strategy plans to incorporate Artificial Intelligence (AI) technology into these services.
- Along with the UAE 2031 AI strategy, the Emirates Blockchain Strategy 2021, the UAE National Innovation Strategy, the UAE National Strategy for Higher Education 2030, and the UAE Centennial 2071 Plan have also enabled the country's rapid digital adoption. Therefore, adopting cybersecurity is expected to witness huge regional demand during the forecast.
- In March 2022, 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.
- With the growing 5G, mobile subscriptions, and total fiber broadband networks in the country, the government, in collaboration with telecommunication companies, is taking initiatives to tackle cyberattacks and improve security standards and practices across the UAE telecom sector. According to the Telecommunications Regulatory Authority (UAE), In June 2022, the number of mobile subscriptions in the United Arab Emirates (UAE) was about 204 subscriptions per hundred inhabitants. The total number of active mobile subscriptions in the UAE reached approximately 18.7 million in that month.

### Retail Industry Vertical is Expected to Hold Significant Market Share

- The retail industry has become a prime target for cyber-attacks, as it handles large amounts of sensitive customer data, including payment card information and personal identification details. According to PPRO, the most popular online payment method in the United Arab Emirates (UAE) in 2023 was by card about 48 percent. As a result, the demand for cybersecurity solutions in the retail sector has increased significantly over the last few years, leading to the growth of the cybersecurity market in the industry.
- Many retailers are moving their operations to the cloud to reduce costs and improve efficiency. However, this shift also increases the risk of cyber-attacks. As a result, retailers are adopting cloud security solutions, such as encryption and access controls, to protect their sensitive data in the cloud.
- However, several retailers have been slow to adopt or invest in cybersecurity measures, either due to a lack of resources or a

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

belief that they are not at risk of being targeted. This has made them vulnerable to cyber-attacks.

- In addition, retailers are using threat intelligence solutions to stay ahead of cyber threats, which provide real-time information on emerging threats, enabling retailers to take action. Thus, as retailers continue to adopt new technologies, the industry's demand for cybersecurity solutions is expected to grow.
- Data is crucial for the retail industry and is derived from the statistics of warehouse inventory, customer traffic patterns, point-of-sale systems, customer surveys, and competitor pricing, among others. Leveraging and drawing meaningful insights from large data sets is critical to forecasting the growth of the retail industry. Thus, breaches lead to customer dissatisfaction, extend downtime, and inflict regulatory penalties.

## UAE Cybersecurity Industry Overview

The UAE Cybersecurity Market fragmented with the presence of major players like IBM, Cisco Systems, Inc., Juniper Networks, Oracle Corporation, and Palo Alto Networks. Players in the market are adopting strategies such as partnerships and acquisitions to enhance their solution offerings and gain sustainable competitive advantage.

- September 2022 - To address misconfiguration in SaaS (Software-as-a-Service) applications, Palo Alto Networks announced innovations in Prisma SASE that allow customers to identify and remediate misconfigurations in SaaS apps using SaaS Security Posture Management capabilities. Palo Alto Networks strengthened its protection for SaaS (Software-as-a-Service) applications and reinforced ZTNA (Zero Trust Network Access) 2.0 with improved capabilities.
- January 2022 - Emirates Integrated Telecommunications Company (EITC) entered into a strategic partnership with IBM, hoping to harness IBM's security and software solutions for EITC's Digital Trust portfolio and Cyber Defense Center.

## 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 Industry Attractiveness - Porter Five Forces

##### 4.2.1 Bargaining Power of Suppliers

##### 4.2.2 Bargaining Power of Consumers

##### 4.2.3 Threat of New Entrants

##### 4.2.4 Intensity of Competitive Rivalry

##### 4.2.5 Threat of Substitutes

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

#### 4.3 Assessment of Impact of COVID-19 on the Market

### 5 MARKET DYNAMICS

#### 5.1 Market Drivers

##### 5.1.1 Stringent Government Regulations for Increasing Adoption of Cybersecurity Solutions

##### 5.1.2 Growing Digitalization and Remote Working

#### 5.2 Market Challenges

##### 5.2.1 Budget Constraints and High Cost of Solutions

### 6 MARKET SEGMENTATION

#### 6.1 By Security Type

##### 6.1.1 Network Security

##### 6.1.2 Cloud Security

##### 6.1.3 Application Security

##### 6.1.4 End-point Security

##### 6.1.5 Wireless Network Security

##### 6.1.6 Other Security Types

#### 6.2 By Component

##### 6.2.1 Hardware

##### 6.2.2 Solution

##### 6.2.2.1 Threat Intelligence and Response

##### 6.2.2.2 Identity and Access Management

##### 6.2.2.3 Data Loss Prevention

##### 6.2.2.4 Security and Vulnerability Management

##### 6.2.2.5 Intrusion Prevention System

##### 6.2.2.6 Other Solutions

##### 6.2.3 Services

##### 6.2.3.1 Professional Services

##### 6.2.3.2 Managed Services

#### 6.3 By Deployment

##### 6.3.1 Cloud

##### 6.3.2 On-premise

#### 6.4 By End-user Industry

##### 6.4.1 Banking, Financial Services and Insurance

##### 6.4.2 Healthcare

##### 6.4.3 Manufacturing

##### 6.4.4 Retail

##### 6.4.5 Government

##### 6.4.6 IT and Telecommunication

##### 6.4.7 Other End-user Industries

### 7 COMPETITIVE LANDSCAPE

#### 7.1 Company Profiles

##### 7.1.1 IBM

##### 7.1.2 Cisco Systems, Inc.

##### 7.1.3 Juniper Networks

##### 7.1.4 Oracle Corporation

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

- 7.1.5 Palo Alto Networks
- 7.1.6 Fortinet, Inc.
- 7.1.7 Microsoft Corporation
- 7.1.8 Trend Micro DMCC
- 7.1.9 Dell Technologies, Inc.
- 7.1.10 Rapid7, Inc.
- 7.1.11 Injazat

## 8 INVESTMENT ANALYSIS

## 9 FUTURE OF THE MARKET

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

## UAE Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 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                          | 2026-03-02 |
|               |  | Signature                     |            |

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)  
[www.scotts-international.com](http://www.scotts-international.com)