United Arab Emirates 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 cybersecurity market in the United Arab Emirates is expected to register a CAGR of 16.4% during the forecast period. The rapid digitalization in the United Arab Emirates has triggered the number of connected devices by opening new gateways for cyberattacks. Cybersecurity has become increasingly imperative for governments and companies as digitization has been gathering pace 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, UAE announced the adoption of 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% 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 the relationship between these countries.
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.
Moreover, in November 2020, the United Arab Emirates Cabinet agreed to establish the UAE Cybersecurity Council to develop a comprehensive cybersecurity strategy and create a safe and robust cyberinfrastructure.
In the previous year, Kaspersky researchers revealed that the United Arab Emirates is one of the most targeted countries in the region when it comes to Advanced Persistent Threats (APT). The researchers worked on 49 investigative reports on 16 cyber gangs actively targeting the UAE since the COVID-19 pandemic. Kaspersky found that these APT groups primarily target the

country's diplomatic and governmental institutions and educational organizations. Other targeted entities include IT companies, financial institutions, healthcare, law firms, the military, and defense.

UAE Cybersecurity Market Trends

Increasing Number of Cyberattacks in the Country

The United Arab Emirates, like other Gulf countries, is a target of cyberattacks by threat actors with political motivations. Such threat actors have historically been nation-state actors or political activist groups, generally focused on causing destruction and damage within the utility and critical infrastructure sectors.
There is an upward trend in state-sponsored actors using malware to gather confidential state-owned information. Cybersecurity experts note that cyber-actors are now targeting research centers and educational institutes. However, government (especially foreign affairs and defense-related organizations) and oil and gas entities remain specific targets. SMEs and local government agencies are also as vulnerable as larger organizations due to the perception that they are likely to have a less robust technical infrastructure and fewer resources to protect themselves from malicious threats.
Ransomware continues to be a significant threat in the UAE, which is in line with global trends. According to various reports, many UAE businesses have experienced a considerable ransomware attack in the last few years, resulting in business interruption and the costs of hiring third-party experts to handle such incidents.
Ransomware attackers that are attacking companies in the country are increasingly deploying pressure tactics where, in addition to encrypting data, they exfiltrate personal or commercially sensitive data from organizations and then extort ransom payments from their victims in exchange for decrypting the information and restoring victims' access to their systems and data.
According to Check Point Research (CPR), a Threat Intelligence division of Check Point Software Technologies Ltd, UAE witnessed a 29% increase in weekly cyber attacks on organizations last year compared to 2020.

New Government Regulations along with Private Sector Participation in Strengthening Cybersecurity

The UAE data protection landscape has witnessed several developments over the last few years that are set to continue. There has been an increased focus on consumer protection issues at the federal level. Accordingly, in June 2020, the Federal National Council approved a draft federal law on consumer protection to ensure increased consumer protection and data security.
Regarding the UAE offshore legal framework (i.e., free zones), the Abu Dhabi Global Market (ADGM) and the Dubai International Financial Center (DIFC) have taken major steps to align with global data protection standards and best practices, especially the EU General Data Protection Regulation (GDPR).
Last year, the recently enacted ADGM Data Protection Regulations repealed the ADGM Data Protection Regulations 2015 and established a more robust and substantive legal framework for protecting personal data.
In addition, organizations that control or process personal data and contravene the ADGM Regulations provisions are subject to administrative fines of up to USD 28 million. This substantially increased from the previous maximum administrative penalty of USD 25,000 under the 2015 regulations.
The Dubai International Financial Center (DIFC) also recently took some significant steps to align with GDPR standards by introducing new Data Protection DIFC Law No. 5 of 2020, which consolidated and replaced previous data protection laws in the DIFC and brought the regime closer in line with international data protection standards. Significant fines have also been introduced, and new obligations on data processors and controllers to notify authorities in case of a breach.

UAE Cybersecurity Market Competitor Analysis

The UAE Cybersecurity Market is fragmented and competitive, comprising several global and regional players. Innovation can bring about a sustainable and competitive advantage to these firms. New fields, such as IoT and Big Data, are reshaping security trends, and the firm concentration ratio is expected to record higher growth during the forecast period. Key players in the market are IBM, Cisco Systems, Oracle Corporation, Palo Alto Networks, and Fortinet.

In 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.

In 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:

United Arab Emirates 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	2026-03-01
		Signature