Security and Vulnerability Management Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 120 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 security and vulnerability management market is expected to register a CAGR of 10% over the forecast period. Organizations in all industries face the challenge of defending against continuous information security breaches. Security professionals are expected to stay ahead of the risks and leverage technologies, policies, and procedures to guard against incoming attacks and protect sensitive data. thus driving the market's growth.

Key Highlights
Also, as organizations accelerate their digital transformation initiatives, they need to quickly make changes to their core business applications without compromising security across on-premise, SDN, and cloud environments. To manage this process, IT and security teams must be able to see the whole network infrastructure and have fine-grained control over it.
According to the Center for Strategic and International Studies (CSIS) and McAfee, cybercrimes, which include damage and destruction of data, stolen money, lost property, theft of intellectual property, and other areas, currently cost the world almost USD 600 billion each year, or 0.8% of global GDP. Such factors are expected to increase the growth of security and vulnerability management software and services.
With the advent of mobile devices and high-speed internet, the BYOD trend is becoming increasingly popular in workplaces. For example, according to Dell, about 60% of employees use a smartphone for work. Such trends are further increasing the market growth for user authentication.
With the increase in the number of devices connected to the internet, the cyber world is expected to see an increase in the occurrence and emergence of new threats and attacks. The WannaCry and Petya attacks, which affected over 150 countries worldwide, have highlighted the vulnerability of devices as endpoints.

Due to the spread of the COVID-19 pandemic, organizations of various sizes have taken initiatives to quickly set up remote working systems to enable employees to work from their homes to protect themselves from infection. This means setting up remote connectivity systems and security apparatuses such as VPNs (Virtual Private Networks), Citrix Virtual Desktop servers, remote desktop connections, file sharing, FTP servers, and several more. This presents some challenges as well as opportunities for the vendors.

Security & Vulnerability Management Market Trends

BFSI Segment is Expected to Hold the Major Market Share

Globally, financial institutions are a top target for cyberattacks. Cybersecurity is becoming more important for financial firms as the majority of financial services are now digital. In this sector, cyberattacks can now target transaction systems and websites, which represents a growing number of attacks. The United States, as one of the world's largest financial markets, is the target of a sizable portion of cyberattacks.
The BFSI sector is faced with several data breaches and cyber-attacks owing to the large customer base that the industry serves. Data breaches result in increased costs for corrective measures and the loss of valuable customer information. For instance, in the recent past, Taiwan's Far Eastern International Bank incurred a loss of around USD 60 million due to malware.
To secure IT processes and systems, secure customer-critical data, and comply with government regulations, private and public banking institutes are focused on implementing the latest technology to prevent cyber-attacks.
With the growing technological penetration, coupled with digital channels such as internet banking and mobile banking, and customers' preferred choice for banking services, banks need to leverage advanced authentication and access control processes. According to IBM, this year, the average cost of a data breach in the financial industry worldwide was USD 5.97 million, up from USD 5.72 million last year.

Asia-Pacific is Expected to Grow at the Fastest Rate

In Asia-Pacific, the frequency of cybersecurity assaults and BYOD data breaches is gradually increasing. The region is, therefore, favorable for the development and need for security and vulnerability management solutions. According to a survey from ESET Enterprise, nearly one in five commercial organizations in this region experienced more than six security breaches in recent years. The major industry participants are concentrating on bolstering their defensive capabilities due to the increased cyberattacks in this area. The countries' governments in this region have also consistently shown interest in this.
Security service applications, such as managed security services, hardware support, consulting, and training, will act as catalysts in the region. There is no indication that the demand for cybersecurity services will decrease, given the rising financial expenses, regulatory costs, and reputational penalties related to cyberattacks. Additionally, according to IBM Security studies, the average cost of a security breach increased to USD 2.71 million per firm across ASEAN. Demand for reliable services has increased significantly as a result of rising costs and a significant increase in ransomware occurrences.
The increasing initiatives by the government and the related regulatory bodies to strengthen security is expected to fuel the adoption of the vendors' solutions over the forecast period. For instance, in May 2021, Microsoft announced its contemplation to unite APAC governments with the cybersecurity council. They stressed the significance of governments collaborating with technology companies to bolster cyber-defense strategies.
Countries like Australia, Indonesia, Japan, Malaysia, the Philippines, Singapore, Sri Lanka, and Thailand are more inclined to adopt security and vulnerability management solutions, as they have detailed and up-to-date cybersecurity strategies in place. These strategies are often backed up by legal and operational frameworks and dedicated agencies that address critical infrastructure protection requirements and emergency response.

On the other hand, countries like Laos, Myanmar, and Pakistan have general information and communication technology (ICT) master plans covering aspects of cybersecurity. This presents an opportunity for vendors to raise awareness about their products in these countries.

Security & Vulnerability Management Market Competitor Analysis

The security and vulnerability management market is moderately competitive and consists of several major players. Players in the market adopt strategies like product innovation, partnerships, and mergers and acquisitions to expand their business footprint. Some of the key developments in the market are:

In October 2022, Microsoft introduced Azure DDoS IP Protection, a new SKU of Azure DDoS Protection for small and medium-sized organizations, and enterprise-grade DDoS protection. DDoS, or distributed denial of service, is a type of assault in which the attacker sends an application more requests than it can handle. This has an effect on the application's accessibility and capacity to serve users. One of the main worries for firms using cloud applications is this kind of attack.

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 INSIGHT
4.1 Market Overview? (Followed by Impact of COVID-19 on the market)
4.2 Industry Attractiveness - Porter's Five Forces Analysis
4.2.1 Bargaining Power of Suppliers
4.2.2 Bargaining Power of Buyers/Consumers
4.2.3 Threat of New Entrants
4.2.4 Intensity of Competitive Rivalry
4.2.5 Threat of Substitute Products
4.3 Industry Value Chain Analysis

5 MARKET DYNAMICS
5.1 Introduction to Market Dynamics?
5.2 Market Drivers?
5.2.1 Increasing Number of Cyber Attacks
5.2.2 Growing Adoption of Cloud Computing by Enterprises
5.3 Market Restraints
5.3.1 Lack of Awareness Toward SVM Solutions

5.3.2 Scalability and Deployment Costs

6 MARKET SEGMENTATION
6.1 By Size of the Organization
6.1.1 Small and Medium Enterprises
6.1.2 Large Enterprises
6.2 By End-user Vertical
6.2.1 Aerospace, Defense, and Intelligence
6.2.2 BFSI
6.2.3 Healthcare
6.2.4 Manufacturing
6.2.5 Retail
6.2.6 IT and Telecommunication
6.2.7 Other End-user Industries
6.3 Geography
6.3.1 North America
6.3.2 Europe
6.3.3 Asia-Pacific
6.3.4 Latin America
6.3.5 Middle East & Africa

7 COMPETITIVE LANDSCAPE
7.1 Company Profiles
7.1.1 IBM Corporation
7.1.2 Qualys Inc.
7.1.3 Hewlett Packard Enterprise Company
7.1.4 Dell EMC
7.1.5 Tripwire Inc.
7.1.6 Broadcom Inc. (Symantec Corporation)
7.1.7 McAfee Inc.
7.1.8 Micro Focus International PLC
7.1.9 Rapid7 Inc.
7.1.10 Fujitsu Limited
7.1.11 Alien Vault Inc.
7.1.12 Skybox Security Inc.

8 INVESTMENT ANALYSIS

9 MARKET OPPORTUNITIES AND FUTURE TRENDS

Security and Vulnerability Management Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 120 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	2026-03-04
		Signature