

Security and Vulnerability Management - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 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 size is estimated at USD 14.45 billion in 2024, and is expected to reach USD 21.65 billion by 2029, growing at a CAGR of 7.5% during the forecast period (2024-2029).

Key Highlights

- The task of defending against the continuous breach of information security lies with organizations in all sectors. Security professionals must continue to keep pace with the risks and leverage technologies, policies, and procedures that safeguard them against an incoming attack and secure sensitive data. This has led to the growth of the market.
- 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.
- As per the Center for Strategic and International Studies 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.
- BYOD trends have become more and more common in workplaces as a result of the advent of mobile devices and high-speed Internet. 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.
- The cyber-world is likely to see an increase in the occurrence and spread of new threats and attacks as more devices are getting connected to the Internet. The WannaCry and Petya attacks, which affected over 150 countries worldwide, have highlighted the vulnerability of devices as endpoints.
- In view of the COVID-19 pandemic, organizations of all sizes have undertaken initiatives for the quick establishment of remote

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

working schemes to enable staff to work from their homes in order to prevent 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 and 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.
- Given the high number of customers served by the BFSI sector, it has been subject to a series of data breaches and cyber-attacks. 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.
- As per IBM, the average cost of data breaches in the finance industry worldwide was USD 5.97 million this year, up from USD 5.72 million last year. Private and public banking institutions are dedicated to the implementation of advanced technologies that will protect them from cyber attacks so as to ensure IT processes and systems, secure customer critical information, and comply with government regulations.
- Banks need to make use of improved authentication and access control procedures in view of the increased penetration of technology, along with digital channels such as Internet and mobile banking, which their customers are more likely to choose than traditional banking services.
- In October 2022, Temenos introduced a SaaS offering that allows banks to manage or handle Financial Crime Mitigation along with composable banking services on a much more reliable, secure, continually evolving, self-service platform. Temenos' FCM-as-a-Service offers pre-built configurations that are aligned with global industry regulations. Banks now have the ability to achieve lower total costs of ownership and improved customer service due to self-provisioning as well as automatic upgrades for rapid compliance and time to value.

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.
- 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. In

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

order to address the critical infrastructure protection and emergency response needs, those strategies are often accompanied by legal and operational frameworks as well as dedicated agencies.

- Conversely, general ICT master plans for cyber security aspects are being prepared in countries such as Laos, Myanmar, and Pakistan. This presents an opportunity for vendors to raise awareness about their products in these countries.

- Moreover, the rising initiatives by the government and the related regulatory bodies to strengthen security are anticipated to fuel the adoption of the vendors' solutions over the forecast period. For instance, in March 2022, in the face of a growing cyber threat landscape across the globe, Australia's Federal Government issued its 2022-23 federal budget with an amount of AUD 9.9 billion (USD 6.39 Billion) to strengthen cybersecurity and intelligence capabilities. The AUD 10 billion (USD 6.46 billion) will be spent under a program called REDSPICE, i.e., Resilience, Effects, Defence, Space, Intelligence, Cyber and Enablers.

Security and Vulnerability Management Industry Overview

The security and vulnerability management market is moderately competitive and consists of several major players. In order to gain a better foothold in the market, players are adopting strategies such as product innovation, partnerships, and mergers and acquisitions.

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.

In April 2022, by extending its strategic alliance with Microsoft, HCL Technologies said it would be able to offer security capabilities to clients all around the world. The Noida-based business has earned each of the four advanced security specializations that Microsoft partners can pursue. The four Microsoft Azure domains that HCL Tech has completed are Identity and Access Management Advanced Specialization, Threat Protection Advanced Specialization, Information Governance and Protection Advanced Specialization, and Cloud Security Advanced Specialization.

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

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

- 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 By 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.

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

8 INVESTMENT ANALYSIS

9 MARKET OPPORTUNITIES AND FUTURE TRENDS

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

Security and Vulnerability Management - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 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	2026-03-02
		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
www.scotts-international.com