Security And Vulnerability Management - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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 Security And Vulnerability Management Market size is estimated at USD 17.24 billion in 2025, and is expected to reach USD 23.5 billion by 2030, at a CAGR of 7.30% during the forecast period (2025-2030).

Key Highlights
- Organizations across various sectors grapple with the challenge of safeguarding against persistent information security breaches. Security professionals, in their relentless pursuit to shield sensitive data, must outpace evolving threats. They harness advanced technologies, enforce robust policies, and implement effective procedures to thwart potential attacks. This proactive stance has catalyzed the market's growth.
- Recently, organizations have increasingly embraced automation to manage vulnerabilities, allowing for more efficient threat identification and prioritization. By harnessing artificial intelligence and machine learning, these entities have drastically reduced the time taken to address and rectify vulnerabilities. Furthermore, as organizations increasingly adopt cloud-based solutions, the demand for robust vulnerability management in these systems intensifies. The rising popularity of containerization technologies, like Docker, underscores the urgent need for enhanced cloud security.
- To adeptly navigate the shifting cyber threat landscape, organizations must elevate security to a top priority. This commitment entails investing in thorough training, cultivating a security-first culture, and understanding that vulnerability management is an ongoing process. Tools such as agent-based scanning, part of the DevSecOps framework, can streamline processes and bolster product security.
- Many organizations, particularly SMEs, still lean on legacy systems and traditional security tools. This dependence has led to fragmented environments, complicating seamless integration. As a result, embedding security and vulnerability management solutions into these complex systems poses a significant challenge. Such obstacles can lead to interoperability issues among tools, restricting security teams' access to real-time data and heightening breach risks. Moreover, this fragmentation can create

information silos, isolating crucial security data across departments and hindering visibility and response.
- Macroeconomic factors play a pivotal role in shaping organizations' approach to security investments. While these entities often grapple with substantial upfront costs for security solutions, spanning software, hardware, training, and integration, economic downturns can shift their priorities. Rising inflation further complicates matters, inflating operational costs and tightening cybersecurity budgets. This financial strain often results in delayed or diminished security upgrades.

Security and Vulnerability Management Market Trends

BFSI Segment is Expected to Hold the Largest Market Share

- Cyberattacks are increasingly targeting financial institutions worldwide. As the financial sector embraces digital platforms, the urgency of cybersecurity becomes paramount. These cyber threats are notably focusing on transaction systems and websites. The United States, a dominant force in the global financial landscape, finds itself at the forefront of these cyber challenges.
- Serving a vast customer base, the BFSI sector has been a frequent target of data breaches and cyberattacks. These breaches not only escalate corrective expenses but also threaten invaluable customer information. In 2024, the Identity Theft Resource Center highlighted 3,158 data compromise incidents in the U.S., affecting over 1.35 billion individuals.
- According to IBM, the global average cost of a data breach in the financial sector rose to USD 6.08 million in 2024, up from USD 5.90 million in 2023. Such escalating costs underscore the growing demand for sophisticated security and vulnerability solutions in the market.
- In their quest for cyber protection, both private and public banks are increasingly adopting advanced technologies. These initiatives not only shield IT processes and vital customer data but also ensure compliance with governmental regulations. As technology adoption surges and preferences shift towards digital avenues like the internet and mobile banking, banks are emphasizing robust authentication and access control, further fueling the demand for security management.
- Banking infrastructure is intricate, intertwining legacy systems, cutting-edge cloud technologies, and a myriad of third-party integrations. Each facet harbors potential vulnerabilities. An overlooked gap can pave the way for a cyberattack, resulting in significant financial and reputational damage. Moreover, banks must navigate stringent regulations, aligning with standards from entities like ISO 27001. Thus, addressing vulnerabilities is not just about data protection; it's a commitment to regulatory compliance and avoiding penalties.

Asia-Pacific is Expected to Witness a Significant Growth

- In the Asia-Pacific region, cybersecurity assaults and BYOD data breaches are increasingly prevalent. This uptick highlights the region's escalating appetite for security and vulnerability management solutions. A survey conducted by ESET Enterprise found that nearly 20% of commercial entities in the Asia-Pacific grappled with more than six security breaches in recent years. In light of the rising cyberattacks, major industry players are bolstering their defenses, a sentiment mirrored by regional governments.
- Security service applications, encompassing managed security services, hardware support, consulting, and training, are set to spearhead growth in the region. As financial, regulatory, and reputational stakes tied to cyberattacks escalate, the appetite for cybersecurity services remains robust. IBM Corporation underscored this urgency, revealing that the average cost of a security breach for firms in ASEAN soared to USD 3.23 million between March 2023 and February 2024. This surge in breach costs, alongside a spike in ransomware incidents, has heightened the demand for reliable cybersecurity services.
- Australia, Indonesia, Japan, Malaysia, the Philippines, Singapore, Sri Lanka, and Thailand are at the forefront of embracing security and vulnerability management solutions, thanks to their robust and up-to-date cybersecurity strategies. These strategies, often reinforced by legal frameworks, operational guidelines, and dedicated agencies, focus on critical infrastructure protection

and emergency response.
- Conversely, nations like Laos and Myanmar are crafting general ICT master plans with an emphasis on cybersecurity. This disparity offers a golden opportunity for vendors to introduce their products in these markets. Moreover, as governments and regulatory bodies intensify their security measures, a notable uptick in the adoption of vendor solutions is on the horizon. IBM Corporation's data reveals that from March 2023 to February 2024, data breaches averaged a cost of USD 4.19 million in Japan, USD 3.62 million in South Korea, and USD 2.35 million in India. Hence, the confluence of such trends and developments is creating a favorable ecosystem for the studied market's growth.

Security and Vulnerability Management Industry Overview

The security and vulnerability management market boasts a diverse landscape, featuring both specialized players and regional conglomerates. While certain high-value segments see dominance from large multinational corporations, a plethora of regional and niche players enrich the competitive tapestry. This vibrant competition stems from the myriad applications of security and vulnerability management, enabling both small and large organizations to flourish.

Prominent players in the security and vulnerability management arena include TQualys Inc., Hewlett-Packard Enterprise Company, Dell EMC, Tripwire Inc., and Broadcom Inc., among others. These companies, backed by strong brand recognition and expansive regional operations, hold a substantial market share. Their competitive strengths lie in innovation, a diverse solutions portfolio, and a solid distribution network. To further their market presence and maintain a competitive edge, these industry leaders actively engage in strategic acquisitions and partnerships.

Success in the security and vulnerability management domain hinges on prioritizing innovation in offerings. As industries increasingly seek advanced solutions, these services are set to become pivotal differentiators. Additionally, expanding service offerings and enhancing customer support will be crucial for fostering enduring relationships and securing repeat business. Companies that invest in emerging markets and tailor their products to regional needs are poised to gain a significant advantage in this fragmented landscape.

Additional Benefits:

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

Table of Contents:

Security And Vulnerability Management - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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	2026-03-06
		Signature