SCOTTS INTERNATIONAL

Cybersecurity Market by Offering, Solution Type, Services (Professional and Managed), Deployment Mode (On-Premises Cloud, and Hybrid), Organization Size (large enterprises and SMEs), Security Type, Vertical and Region - Global Forecast to 2028

Market Report | 2024-01-30 | 639 pages | MarketsandMarkets

AVAILABLE LICENSES:

- Single User $7150.00
- Multi User $8500.00
- Corporate License $9650.00
- Enterprise Site License $11000.00

Report description:

The global cybersecurity market size is projected to grow from USD 190.4 billion in 2023 to USD 298.5 billion by 2028 at a CAGR of 9.4% during the forecast period. The market growth in cybersecurity is fueled by factors driven by increased target-based cyber-attacks, protection of business assets from growing threats, rising IoT trends and the growing need for automated cybersecurity, growing demand for cyber-savvy boards, and complying with government regulations and requirements.
"By offering, the services segment will grow at the highest CAGR during the forecast period."
In the cybersecurity market, by offering, the services segment is anticipated to grow at the highest CAGR due to a combination of factors. As cyber threats become increasingly sophisticated, there is a growing demand for expert services that provide advanced protection and mitigation strategies. It includes a need for continuous monitoring, threat intelligence, and incident response, which specialized cybersecurity services effectively deliver. Moreover, organizations undergoing digital transformation often lack the in-house expertise required to manage complex cybersecurity landscapes. The gap is being filled by external cybersecurity service providers, who offer tailored solutions and support.
Furthermore, the evolving regulatory landscape across various industries necessitates ongoing compliance and risk management, areas where cybersecurity services play a critical role. These services help organizations protect against cyber threats and ensure they remain compliant with changing regulations. The demand for specialized knowledge, coupled with the growing complexity of cyber threats and compliance requirements, drives the rapid growth of the services segment in the cybersecurity market.

"By vertical, the BFSI segment will grow at the largest market size during the forecast period."

The BFSI sector is anticipated to hold the largest market size in the cybersecurity market among various verticals. Its prominence is due to the sector's handling of highly sensitive and valuable financial data, making it a prime target for cyberattacks. Financial institutions are under constant threat from a range of sophisticated cyber threats like phishing, malware, and ransomware, driving the need for robust cybersecurity measures. Moreover, the BFSI sector is heavily regulated, with stringent data protection and privacy laws requiring strong security protocols to ensure compliance and avoid heavy penalties. The rapid shift towards digital banking and online financial services further escalates the risk of cyber threats, necessitating advanced cybersecurity solutions to protect customer data and maintain trust. The combination of these factors - high-value targets, stringent regulations, and the increasing digitization of financial services - contributes to the BFSI vertical commanding the largest market size.

"North America is expected to account for the largest market size during the forecasted period."
The North American region is anticipated to dominate the cybersecurity market in terms of market size, primarily due to several contributing factors. The North American region, particularly the US, is home to numerous leading technology and cybersecurity companies, fostering a strong market for cybersecurity solutions. Additionally, North America experiences a high volume of cyber threats, which drives the demand for advanced cybersecurity measures. The region also has stringent regulatory frameworks and data protection laws, such as GDPR and CCPA, compelling organizations to invest in robust cybersecurity infrastructures to maintain compliance. Moreover, the widespread adoption of digital technologies, including cloud services and IoT devices, in finance, healthcare, and government sectors further elevates the need for comprehensive cybersecurity solutions. The combination of a technologically advanced landscape and a high incidence of cyber threats positions North America as a leader in the global cybersecurity market.

"Asia Pacific is anticipated to account for the highest CAGR during the forecasted period."
The Asia Pacific region is anticipated to exhibit the highest CAGR in the cybersecurity market, a trend driven by several factors. Rapid economic growth in the Asia Pacific region led to a surge in digital transformation across businesses and government sectors, significantly increasing the need for robust cybersecurity measures. The growth is accompanied by a substantial rise in internet usage and mobile connectivity, expanding the potential for cyber threats. Furthermore, countries in the Asia Pacific are progressively implementing stricter data protection regulations, pushing organizations to strengthen their cybersecurity infrastructure. Additionally, as key sectors like finance, healthcare, and retail increasingly embrace digital technologies, their vulnerability to cyberattacks grows, driving the demand for advanced cybersecurity solutions. A combination of digital growth, regulatory changes, and heightened threat awareness contributes to the high projected growth rate in the cybersecurity market in the Asia Pacific region.

Breakdown of primaries
The study contains insights from various industry experts, from suppliers/software developers to OEMs and Tier 1 vendors.
The break-up of the primaries is as follows:
-By Company Type: Tier 1 - 25%, Tier 2 - 40%, and Tier 3 - 35%
-By Designation: C-level - 30%, Directors - 35%, and Others- 35%
-By Region: North America - 15%, Europe - 25%, Asia Pacific - 30%, Latin America - 20%, Middle East & Africa - 10%
The key vendors in the global cybersecurity market include IBM (US), Cisco (US), Microsoft (US), Palo Alto Networks (US), Fortinet (US), Check Point (US), Trellix (US), Trend Micro (Japan), Rapid7 (US), Micro Focus (Open text) (UK), AWS (US), Oracle (US), Accenture (Ireland), CyberArk (US), SentinelOne (US), Qualys (US), F-secure (Finland), F5 (US), RSA Security (US), Sophos (UK), Forcepoint (US), Proofpoint (US), Juniper Networks (US), SonicWall (US), Zscaler (US), Google (US), Fortra (US), Crowdstrike (US), Broadcom (US), Redington (India), NTT (Japan), Algosec (US), Cynet (Israel), Nozomi Networks (US), Revbits (US), Aristi Labs (India), Illumio (US), Seclore (US), Securonix (US), Sejel Tech (SaudiArabia), Proficio (US), Wijungle (India), Secureden (US), Orca Security (US), Wattle Corporation (India), Open Raven (US), CPX (UAE), and Mesh Security (Israel).
The study includes in-depth competitive intelligence covering company profiles, recent developments, and key market strategies.
Research Coverage
The report segments the cybersecurity market and forecasts its size by offering (solution and services), solution type (IAM,

antivirus/antimalware, log management & SIEM, firewall, encryption & tokenization, compliance & policy management, patch management, and others), services (professional and managed), deployment mode (on-premises, cloud, and hybrid), organization size (large enterprises and SMEs), security type (network security, endpoint & IoT, cloud security, and application security), verticals (BFSI, government, IT & ITeS, healthcare & life science, aerospace & defense, retail & eCommerce, manufacturing, energy & utilities, telecommunication, transportation & logistics, media & entertainment, and other verticals), and region (North America, Europe, Asia Pacific, Middle East & Africa, and Latin America).

Key Benefits of Buying the Report

The report will help the market leaders/new entrants with information on the closest approximations of the revenue numbers for the cybersecurity market and the subsegments. The report will help stakeholders understand the competitive landscape and gain more insights to position their businesses better and plan suitable go-to-market strategies. The report also helps stakeholders understand the market pulse and provides information on key market drivers, restraints, challenges, and opportunities.

The report provides insights on the following pointers:

-Analysis of key drivers (Increased target-based cyber-attacks to draw operational disruptions, protection of business assets from growing threats, Cybersecurity Mesh Architecture (CSMA) to simplify security infrastructure, Rising IoT Trends and the growing need for automated cybersecurity, Growing demand for cyber-savvy boards, and Complying with government regulations and requirements), restraints (Lack of skilled cybersecurity professionals and lack of budget among SMEs and start-ups in developing economies), opportunities (Adoption of cloud-based cybersecurity solutions among SMEs, Growth of endpoint security segment due to increased BYOD trend, Enhancing Cybersecurity with AI), and challenges (Deploying and implementing cybersecurity design solutions, Diverse nature of sophisticated threats, Complexities of vendor overload and multiplicity of technologies, Difficulties in addressing the complexity of advanced threats).

-Product Development/Innovation: Detailed insights on upcoming technologies, research & development activities, and product & service launches in the cybersecurity market.

-Market Development: Comprehensive information about lucrative markets - the report analyses the cybersecurity market across varied regions.

-Market Diversification: Exhaustive information about new products & services, untapped geographies, recent developments, and investments in the cybersecurity market.

-Competitive Assessment: In-depth assessment of market shares, growth strategies, and service offerings of leading players like IBM (US), Cisco (US), Microsoft (US), Palo Alto Networks (US), Fortinet (US), Check Point (US) among others in the cybersecurity market strategies

Table of Contents:

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com

SCOTTS INTERNATIONAL

Cybersecurity Market by Offering, Solution Type, Services (Professional and Managed), Deployment Mode (On-Premises Cloud, and Hybrid), Organization Size (large enterprises and SMEs), Security Type, Vertical and Region - Global Forecast to 2028

Market Report | 2024-01-30 | 639 pages | MarketsandMarkets

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	$7150.00
	Multi User	$8500.00
	Corporate License	$9650.00
	Enterprise Site License	$11000.00
	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*	

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com

Zip Code*		Country*	
		Date	2025-05-20
		Signature	