SCOTTS
INTERNATIONAL

Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 237 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 size is estimated at USD 203.78 billion in 2024, and is expected to reach USD 350.23 billion by 2029, growing at a CAGR of 11.44% during the forecast period (2024-2029).

Cybersecurity protects the network, information, and personal data from cyberattacks. The trends of BYOD, AI, IoT, and machine learning in cybersecurity are rapidly growing. For instance, machine learning offers advantages in outlier detection, which benefits cybersecurity.

Key Highlights
-The cybersecurity industry ecosystem comprises several regional clusters of cybersecurity firms contributing to global market dynamics. In the current market scenario, the cybersecurity industry operates in three distinct mega-clusters: the San Francisco Bay Area (SFBA), Metropolitan Washington, DC, and Israel.
-The three cybersecurity mega-clusters share two essential characteristics. The first is that the startup and high-tech innovation culture is a significant growth driver for all three ecosystems. SFBA and Israel have thriving startup ecosystems with a substantial associated flow of risk capital. They are heavily focused on products, while Washington exhibits a higher proportion of service-based firms (in Washington, only 11% of cybersecurity firms are focused solely on products). The second characteristic is the link between human capital and national security.
-Ransomware attacks have ravaged many state and local public sector agencies. In some cases, entire local governments were forced to declare an emergency due to massive leaks of sensitive data and loss of services. For instance, in June 2021, JBS Foods, the world's leading meatpacking enterprise, declared that it had paid a USD 11 million ransom to REvil ransomware threat actors following a cyberattack that forced the company to shut down production at several sites worldwide, including its production facilities in United States, Australia, and Canada.

-One of the major causes of growing cyberattacks is the lack of skilled cybersecurity personnel in each industry. The number of experienced cybersecurity professionals, especially in Europe, Asia-Pacific, Latin America, and the Middle-East, is low compared to the need for security professionals to handle cyber threats for financial institutes, government organizations, and private sector/industrial businesses.
-Due to the ongoing COVID-19 pandemic, countries worldwide have implemented preventive measures. With schools being closed and communities being asked to stay at home, multiple organizations have found a way to enable their employees to work from their homes. This has, thus, resulted in a rise in the adoption of video communication platforms.

Cybersecurity Market Trends

The Cloud Segment to Witness Significant Growth

- The increasing realization among enterprises about the importance of saving money and resources by moving their data to the cloud instead of building and maintaining new data storage drives the demand for cloud-based solutions. Owing to multiple benefits, cloud platforms and ecosystems are anticipated to serve as a launchpad for the explosion in the pace and scale of digital innovation over the next few years.
- Cloud-based solutions also benefit from lower capital expenditure requirements, making them much more compelling. Deploying cloud-based services can significantly reduce the Capex requirements as companies need not invest in hardware components. Cloud solutions also enable better prediction of the cost of an application, and companies don't incur much upfront cost to incorporate the technology. Also, the hardware and IT support savings make cloud-based solutions much more affordable.
- Companies that are considering moving from on-premise software to cloud-based solutions are primarily checking the potential solutions for their key security features, including standards compliance and intrusion prevention and detection.
- In October 2022, Google Cloud declared a significant expansion of its trusted cloud ecosystem. It highlighted new integrations and offerings with more than twenty partners, focusing on enabling greater data sovereignty controls, supporting Zero Trust models, unifying identity management, and improving endpoint security for global businesses.
- Cloud technology provides organizations with the flexibility they need to increase and decrease their bandwidth with the needs of their operations. This approach can cut costs and give businesses an edge over the competition.

North America is Expected to Hold Major Market Share

- Cybersecurity has become an increasingly important area of focus in the United States in recent years due to the growing number of cyber threats and attacks that organizations and individuals face. According to the Identity Theft Resource Center, the number of data compromises and individuals impacted in the United States in 2022 was 1,802 and 422.14 million, respectively.
- The increasing frequency and sophistication of cyber-attacks are driving the adoption of cybersecurity solutions in the United States. Moreover, the growing regulatory requirement leads many organizations to adopt and invest in cybersecurity solutions, as many industries in the United States are subject to regulations such as HIPPA, GDPR, and PCI DSS.
- Education, the public sector, universities, healthcare, and municipalities were among the major sectors affected by cyber-attacks in terms of data breaches and ransomware in the United States in 2022. There has been significant investment in cybersecurity research and development in the United States. The United States government is allocating a large number of funds. For instance, in April 2022, the United States Department of Energy (DOE) announced that it would invest USD 12 million in six new research, development, and demonstration (RD&D) projects to develop innovative cybersecurity technology to ensure that energy delivery systems are designed, installed, operated, and maintained to survive and recover quickly from cyberattacks.
- In Canada, cybercrime is rapidly gaining traction, and the impact is increasing alarmingly. According to the Ministry for

Government Digital Transformation, Quebec, around 3,992 provincial government websites, including those related to health, education, and public administration, can be at risk.
- In order to support the development of a strong national cyber security ecosystem, the Minister of Innovation, Science and Industry announced that the National Cybersecurity Consortium (NCC) received up to USD 80 million to lead the Cyber Security Innovation Network (CSIN) in February 2022. This funding was crucial to foster a strong national cyber security ecosystem in Canada and position the country as a global leader in cyber security.

Cybersecurity Industry Overview

The cybersecurity market comprises several global and regional players vying for attention in a fairly contested market space. Although the market poses high barriers to entry for new players, several new entrants have been able to gain traction. Crowdstrike Holdings Inc., Check Point Software Technologies Ltd, Cisco Systems Inc., Cyberark Software Ltd, and Dell Technologies Inc. are major players in the market.

- In February 2023, Check Point Software Technologies Ltd announced the introduction of Check Point Horizon XDR/XPR, a cooperative cybersecurity solution. It effectively protects organizations against developing cyber threats by smartly correlating data and trying to thwart attacks across all vectors, reducing the impact of threats and making it simple for supervisors and analysts to comprehend and respond to incidents.
- In December 2022, CrowdStrike announced the development of the CrowdStrike Falcon platform to give the sector's finest adversary-driven external attack surface management (EASM) solution for better adversary intelligence and real-time internet access detection. CrowdStrike Falcon Surface, a standalone module featuring abilities from the recent acquisition of Reposify, was announced as part of the platform update.

Additional Benefits:

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

Table of Contents:

SCOTTS INTERNATIONAL

Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 237 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	2026-03-03
		Signature	

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