Cybersecurity Software 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 cybersecurity software market is expected to register a CAGR of 12.5% during the forecast period. The cybersecurity market is primarily driven by the upswing in cyberattacks happening in various end-user industries. Further, with the growing digitalization, cyberattackers are inventing new ways to conduct cyberattacks; such factors are expected to boost the demand for cybersecurity solutions in the country.

Key Highlights
Cyber security software, often known as computer security software, is used to secure and protect computers, networks, and other computing devices. Because of their extensive overlap and the adage that the best defence is a good attack, this is generally used in defending computer systems or data but can also include programs intended expressly for subverting computer systems.
Cyber security software assists in managing to access control, the system's protection against viruses, malware, and illegal access, the safety of data, and the defence against other system-level security concerns. Anti-virus software, internet security software, malware/spam ware removal, firewall software, network security software, protection software, and many other forms of cyber security software are available. The growing popularity of digitalization drives the expansion of the cybersecurity software market.
Cyber security is critical because the government, military, business, financial, and medical entities acquire, process, and store massive amounts of data on computers and other devices. A considerable amount of such data may contain sensitive information, such as intellectual property, financial data, personal information, or different sorts of data whose unlawful access or exposure could have adverse effects.
The major factors driving the Cyber Security Software Market are an increase in the frequency and sophistication of cyber-attacks, the emergence of disruptive digital technologies such as IoT, stringent data protection regulations for information security, and an

increase in the number of supply chain-based attacks that target the software supply chain. Massive cyber attacks are becoming more common around the world.
Furthermore, Technologies such as the Internet of Things (IoT) and new business models rely heavily on global digitalization for success. As the system becomes more complicated, networked, and handles more information, the attack surface expands, revealing holes in the business's security system. These instances create a massive demand for cybersecurity software services.
One of the major causes of growing cyberattacks is the lack of skilled cybersecurity personnel in each industry. Experienced cybersecurity professionals, especially in Europe, Asia-Pacific, Latin America, and the Middle East, are less than the need for security professionals to handle the cyber threats for financial institutes, government organizations, and private sector/industrial businesses.
Innovation can bring about a sustainable, competitive advantage. New markets like Big Data or the IoT are reshaping their security trends. The firm concentration ratio is expected to record higher growth during the forecast period because several software firms look at this market as a lucrative opportunity to consolidate their offerings.
For instance, In February 2022, Palo Alto Networks inc. announced the launch of Cortex XSIAM, an AI-driven platform to transform how analytics, data, and automation are deployed in the organization's security. It will offer a modern alternative in today's threat landscape.
The pandemic has further accelerated the need for cybersecurity as enterprises planning to execute months-long business continuity plans (BCP), including information security monitoring and response while operating under quarantine conditions, focused on enhancing cybersecurity. Also, the demand for the cybersecurity software market is rising in the post-pandemic scenario.
Government agencies are allotting strategic funds to strengthen their digital interface in the post-pandemic era. For instance, In 2021, following recent hospital breaches, French President Emmanuel Macron announced a plan to invest EUR 1 billion (USD1.2 billion) to strengthen cybersecurity in France, with EUR350 million (approx. USD 400 million USD) set aside for hospitals.

Cybersecurity Software Market Trends

The BFSI End-User Segment is Expected to Witness Significant Growth

The BFSI industry is one of the critical infrastructure segments that face multiple data breaches and cyber-attacks, owing to the massive customer base that the sector serves and the financial information that is at stake. As a highly lucrative operation model with phenomenal returns and the added upside of relatively low risk and detectability, cybercriminals are optimizing various diabolical cyberattacks to immobilize the financial sector. These attacks' threat landscape ranges from Trojans, ATMs, ransomware, mobile banking malware data breaches, institutional invasion, data thefts, fiscal breaches, etc.
Public and private banking institutes are focusing on implementing the latest technology to prevent cyber attacks with a strategy to secure their IT processes and systems, secure customer critical data, and comply with government regulations. Besides, banking institutions are pushed to adopt a proactive security approach with greater customer expectations, rising technological capabilities, and regulatory requirements. With the growing technological penetration and digital channels, such as internet banking, mobile banking, etc., online banking has become customers' preferred choice for banking services. There is a significant need for banks to leverage advanced authentication and access control processes.
In February last year, the Department of Justice (DoJ) and industry group Bankers Association of the Philippines (BAP) signed a memorandum of understanding (MoU) to raise cybersecurity awareness and combat cybercrime in the Philippines. The BAP aims to strengthen the banking industry's cyber-resilience and develop a collaborative partnership with the Justice Department to achieve a coordinated, collective, and strategic cyber response through information sharing and collaboration in the wake of rising cybercrime incidents in the country.
In the last year, financial firms worldwide were impacted by innovative new ransomware tactics that maximized ROI for the threat actors. While financial firms represent a small percentage of victims directly targeted by ransomware attacks, they can and have

been impacted by attacks on third parties, who are prime targets. Such threats are poised to increase the usage of cybersecurity software services in the BFSI sector.
Over the past few years, several technology start-ups specializing in the financial segment have emerged, disrupting how they make purchases. For instance, in India, from app-based wallets and Aadhaar/UPI-linked instant transactions to single-window e-commerce apps, fintech start-ups need to be mindful of the threats and invest in creating a robust data security framework for the apps. This needs to be addressed as these may be boot-strapped start-ups and generally avoid the hefty investment required for a more than essential digitally secure ecosystem. This needs to be addressed by collaboration with cybersecurity firms that provide customized and value-driven services against the big-budget packages.

North America is Expected to Hold Significant Share

North America is presumed to be the most significant revenue-generating region, as there is a particular focus on innovations in the US and Canada. These nations have the world's most competitive and quickly changing consumer data platform markets. A higher rate of infrastructure growth and the massive growth of data from all industry verticals are expected to make North America one of the top potential markets for growth.?
The presence of significant cybersecurity software providers with headquarters in North America also drives the market growth in this region.
Healthcare cybersecurity crimes are on the rise in the US and continue to be one of the major concerns in the country, fueling firms to drive solutions in the market.
The Health Insurance Portability and Accountability Act, a federal statute of the United States, reported the increase of breaches by 25% year-over-year in 2020 in the Healthcare Data Breach Report published in January last year, with 29,298,012 healthcare records breached.
Increased investments in the industry mark the country for cybersecurity solutions and cyber threat-detecting software and platforms. With the increased awareness amongst companies spanning from small to large enterprises, US companies are deploying stricter solutions to protect data and installing fraud and threat detection programs to find risks at an earlier stage to respond at an earlier stage driving the injection of funds into the industry. For instance, Horizon3.ai, a cybersecurity company based in California, raised an investment of USD 5 million in the Series A round of investment which SignalFireled.
In Canada, cybercrime is rapidly gaining traction, and the impact is increasing at an alarming rate. In December 2021, Ministry for Government Digital Transformation, Quebec, revealed that they would shut down close to 4,000 government websites following the threat of an international cyberattack on a widely used logging system. According to the ministry, around 3,992 provincial government websites could be at risk, including those related to health, education, and public administration.

Cybersecurity Software Market Competitor Analysis

The global cybersecurity software market is highly fragmented and competitive, comprising several international and regional players. Innovation can bring about a sustainable, competitive advantage to these firms. New fields, such as Big Data and IoT, are reshaping security trends, and the firm concentration ratio is expected to record higher growth during the forecast period. Key players in the market are Cisco Systems Inc., Microsoft Corporation, IBM Corporation, and a few others.

April 2022 - CrowdStrike and Mandiant have established a strategic alliance to help joint customers investigate, remediate, and defend against increasingly sophisticated cybersecurity events that impact enterprises worldwide. Mandiant will use the CrowdStrike Falcon platform and subscription options for its incident response (IR) services and proactive consulting engagements for joint customers as part of the agreement.

February 2022 - Check Point Software Technologies has acquired Spectral, a key innovator in developer-first security tools. This acquisition will help the company to extend its cloud solutions, Cloud Guard, with developers' first security platform and provide the broadest range of cloud application security use cases.

Additional Benefits:

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

Table of Contents:

Cybersecurity Software 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	2026-02-27
		Signature