Cloud Security Software - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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 Cloud Security Software Market size is estimated at USD 53.72 billion in 2025, and is expected to reach USD 120.64 billion by 2030, at a CAGR of 17.56% during the forecast period (2025-2030).

Key Highlights
- The growing data generation and increasing complexity of technologies have resulted in a heavy dependence of organizations on cloud services for operations and data management. This growth in the adoption of cloud services directly impacts the demand for cloud security solutions.
- Cloud technology and cloud-based resources help mitigate the rise in lethal cyber-security threats. Cloud security requires a set of policies and controls vital for the security of applications, infrastructure, and data. Threats, such as data loss, breaches, and insecure application programming interfaces (API), are frequent on the cloud computing platform. The evolution of the cyber environment and related technologies paved the way for new threats. Cyber-attacks are highly targeted, persistent, and technologically advanced.
- 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. Cybercriminals are leveraging an abundance of harmful cyberattacks to immobilize the financial industry since it is a highly lucrative operating model with the added benefit of relatively low risk and detectability. These attacks' threat landscape ranges from Trojans, malware, ATM malware, ransomware, mobile banking malware, data breaches, institutional invasion, data thefts, fiscal breaches, etc.
- Vendors offering security solutions are actively involved in collaborating with other managed security service providers. For instance, in October 2022, Google Cloud declared a significant extension of its trusted cloud ecosystem. It highlighted new integrations and offerings with more than twenty partners focused on enabling more excellent data sovereignty controls, assisting Zero Trust models, unifying identity management, and improvising endpoint security for global businesses.

- However, factors like integrating various complexities with legacy infrastructure could limit the market's overall growth throughout the forecast period.
- Due to the outbreak of COVID-19, the cloud security market grew significantly. It was expected to witness massive growth during the post-COVID-19 period as cloud-based services and tools were increasingly adapted due to organizations deploying remote work access amid lockdowns in different countries. The rise in the usage of cloud-based services during this pandemic became a hotspot for cyberattacks as millions worked in unfamiliar, less secure circumstances. Thus, a cloud security solution played a vital role during this pandemic and is expected to witness a surge.

Cloud Security Software Market Trends

Healthcare Sector to Witness the Significant Growth

- Healthcare organizations have become more distributed, owing to remote clinical offices, trial sites, rehab facilities, outsourcing, and off-site workers, leading each office and individual to require unique yet seamless access to applications and resources via various devices. Healthcare organizations recognize the benefits provided by cloud technology, such as greater flexibility, scalability, and availability of systems and applications.
- With advancements in healthcare, such as electronic medical records and other patient details being registered with the respective hospitals, the potential vulnerability for the data has been increasing, owing to which the implementation of network security has been of primary importance.
- Using AI, data-driven security monitoring, and behavioral analytics makes cloud-based security more effective. For instance, Microsoft's integrated intelligent security graph collects billions of data points daily and uses machine learning and AI to analyze and identify evolving cybersecurity attacks.
- In April 2022, the U.S. Food and Drug Administration published a draft guidance, Cybersecurity in Medical Devices, Content of Premarket Submissions and Quality System Considerations, regarding medical device cybersecurity. The draft guidance emphasizes safeguarding medical devices throughout a product's life cycle. These recommendations can enable an efficient premarket review process and help assure that marketed medical devices are sufficiently resilient to cybersecurity threats.
- According to May 2023 Healthcare Data Breach Report, most of the month's data breaches were hacking IT incidents, many of which were ransomware attacks and data theft or extortion attempts. Around 81.33% of the month's data breaches were hacking, and IT incidents, and those incidents accounted for approximately 99.54% of all breached records. The protected health information of about 18,956,101 individuals was exposed or stolen in those incidents. The average data breach size was 310,756 records, and the median breach size was 3,833.

The Asia-Pacific to Witness the Highest Growth

- Due to the rise in the usage of various IoT devices and the increasing scope and speed of digital transformation in the Asia-Pacific region, the current network infrastructure is becoming widely exposed to cyberattacks. Social media, internet, and mobile users have all seen a drastic rise in recent years, contributing to the region's strong growth in cybersecurity. This is expected to fuel the market growth opportunity within the region throughout the forecast period.
- Moreover, the region's various governments are imposing new cybersecurity laws to reduce the impact of cyber phishing, malware, and other cybersecurity threats. For instance, South Korea's ICT ministry announced the plan to spend KRW 670 billion (USD 607 million) by 2023 to bolster the country's cybersecurity capabilities to respond to growing new digital threats. The country plans to develop infrastructure to quickly respond to cybersecurity threats by collaborating with major cloud and data center companies to collect threat information in real time, compared to the current system that relies on individual reports.

- Recently, there have been multiple attacks on Indian power grids by China. In April 2022, India's power sector was targeted by hackers in a long-term operation. The group primarily utilized the trojan ShadowPad, which is believed to have been developed by the contractors for China's Ministry of State Security.
- Also, due to the rise in technological advancements, there is an increase in the number of connected devices in China. It is a significant Internet of Things (IoT) market globally. Furthermore, 5G and 5G-enabled devices exponentially increase the devices' interconnectivity. As a result, it increases the overall adaptability of the connected devices, thereby directly augmenting the need for security products in the market. Moreover, the websites are thereby prone to be manipulated and impersonated by third parties, and sensitive user data communicated with the website can be intercepted more easily by foreign intelligence agencies.
- In July 2023, Sangfor Technologies Co., Ltd., a provider of IT infrastructure solutions specializing in Cloud Computing & Network Security, and Cloudsec Asia Co., Ltd., a provider of cloud security and cyber security services in Thailand, formed a strategic partnership primarily to deliver comprehensive managed services for cyber threat detection. The collaboration between Sangfor Technologies and Cloudsec Asia targets to address the rising demand for effective cyber threat management within business organizations. By leveraging their expertise, the companies would deliver a managed service that empowers organizations to proactively mitigate and detect cyber threats while overcoming challenges like time constraints, limited resources, and technological complexities associated with cybersecurity management.

Cloud Security Software Industry Overview

The market for cloud security software is fragmented due to the rise in cyber-attacks over the years. Enterprises have become more aware and careful regarding their data stored in the cloud. Thus, they offer offerings from NortonLifeLock Inc. (Broadcom Inc.), CA Technologies (Broadcom Inc.), Microsoft Corporation, Armor Defense Inc., etc.

In April 2023, Uptycs, the provider of the first unified CNAPP and XDR platform, declared the ability to collect and analyze GitHub audit logs and user identity information from Okta and Azure Active Directory to reveal suspicious behavior as the developer moves code in and out of repositories and into production. The result is an "early warning system" that enables the security teams to identify and stop threat actors before they can access the cloud's crown jewel data and services.

Additional Benefits:

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

Table of Contents:

Cloud Security Software - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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	2025-05-06
		Signature