+357 96 030922
info@marketpublishers.com

Cloud Workload Protection Market Assessment, By Enterprise Size [Large Enterprises, Small & Medium Enterprises], By Services [Professional Services, Managed Services], By Deployment Mode [Public Cloud, Private Cloud, Hybrid Cloud], By End-use Industry [BFSI, Healthcare, Education, Retail, Government, Others], By Region, Opportunities and Forecast, 2016-2030F

https://marketpublishers.com/r/C16AA0468FB7EN.html
Date: March 2025
Pages: 246
Price: US$ 4,500.00 (Single User License)
ID: C16AA0468FB7EN

Abstracts

Cloud workload protection market has experienced significant growth in recent years and is expected to maintain a strong pace of expansion in the coming years. With projected revenue of approximately USD 5.32 billion in 2022, the market is forecasted to reach a value of USD 27.15 billion by 2030, displaying a robust CAGR of 22.6% from 2023 to 2030.

Cloud workload protection improves the security of cloud-based digital assets. It detects threats in real-time, updates security measures automatically, and assures compliance. It means it aids in preventing data breaches, simplifies security administration, keeps your organization functioning smoothly, and preserves the privacy of the data. It is like a powerful cloud defense against cyber-attacks.

The cloud workload protection market is expanding significantly as more businesses use cloud computing and modernize their operations, implying that there are more potential consumers for security services. As cyber threats become more sophisticated, businesses recognize the need for solid security, prompting them to invest in cloud protection. Finally, rules drive organizations to upgrade their security, which helps drive

+357 96 030922
info@marketpublishers.com

industry growth.

Cloud computing use is increasing in the financial services sector, with 98 percent of businesses adopting some cloud services, a considerable increase from 91 percent in 2020. This trend demonstrates the industry's increased reliance on cloud technology for mission-critical services and regulated data management. However, the adoption rate is determined by cloud service providers' ability to meet security and operational standards while complying with regulatory requirements, reflecting the industry's emphasis on maintaining a secure and compliant cloud environment.

For instance, in July 2023, Palo Alto Networks recently established a new cloud location in Poland, allowing clients to gain local access to sophisticated cybersecurity technologies, such as Prisma Access, Cortex XDR, Cortex XSIAM, sophisticated WildFire, and Cortex Data Lake, while meeting data residency rules.

Escalating Cybersecurity Risks

In today's digital world, cybersecurity faces a constant challenge in the cloud workload protection market as cyberattacks become more frequent and sophisticated. The growing threat emphasizes the need for better security measures to protect cloud workloads. Cloud systems are attractive targets for cybercriminals because they store important data and essential applications. These threats range from ransomware to data breaches and cyber reconnaissance by governments. To counter these risks, organizations are adopting advanced cloud workload protection solutions. These solutions use smart methods to detect threats, monitor systems in real time, and take proactive action to stop attacks. Protecting data and keeping businesses running smoothly is crucial, which is why investing in cloud workload protection has become vital for companies in today's cloud-centric world.

For example, in June 2023, Check Point Software Technologies Ltd. collaborated with TELUS to create TELUS CSPM in Canada, which provides real-time cloud security posture monitoring to protect enterprises from emerging cyber threats and vulnerabilities.

Ensuring Safety Across Diverse Cloud Platforms

Many businesses use numerous cloud services, known as a multi-cloud approach. It enables businesses to be more adaptable and efficient. However, it complicates security. These businesses want specialized solutions that interact with cloud services

+357 96 030922
info@marketpublishers.com

to keep things safe.

As a result, the market for cloud security products is increasing. Companies seek technologies that can protect their data and systems across cloud providers. This forces companies that manufacture these tools to introduce new and better ways to keep things safe. As a result of the increased demand for good cloud security technologies, the cloud workload protection market for these tools is expanding and becoming more essential.

For example, in May 2023, Check Point unveiled the integration of its Next-Generation Cloud Firewall with Microsoft Azure Virtual WAN to improve security in multi-cloud scenarios. This collaboration addresses the growing need for secure cloud communication as cyberattacks on the cloud expand.

Dominance of Hybrid Cloud

Hybrid cloud is the market leader in cloud workload protection market due to its unique combination of flexibility and security. Organizations are increasingly turning to hybrid architectures to balance the benefits of public and private clouds as it allows to keep vital data on private infrastructure while taking advantage of public cloud scalability. This combination necessitates strong security, making workload security paramount. Hybrid cloud security solutions address these disparities by offering consistent protection across many settings. As businesses embrace digital transformation, the hybrid cloud's capacity to adapt to changing workloads while ensuring data integrity places it as a cloud workload protection market leader.

For instance, in July 2023, Palo Alto Networks deployed a CI/CD Security module to Prisma Cloud's CNAPP platform to safeguard software delivery pipelines, improving overall security for the engineering ecosystem.

North America to Dominate the Market

North America is a prominent region in the cloud workload protection market. It serves as a nexus for technological businesses and cybersecurity professionals, resulting in the development of new and innovative solutions. Many North American businesses and government organizations adopted cloud technology early on to cater the need for robust security to safeguard their data and the data protection laws and regulations compel them to utilize modern security tools. Furthermore, as cyberattacks get more sophisticated, North American companies invest heavily in the best security solutions.

+357 96 030922
info@marketpublishers.com

For instance, in August 2023, Wiz launched support for Google Cloud's Vertex AI, allowing customers to securely construct, deploy, and scale machine learning models. Wiz's security capabilities include monitoring AI infrastructure for misconfigurations, data leakage, data poisoning, and other dangers related to AI/ML installations.

Government Initiatives

The United States Defense Department is accelerating cloud computing use and adoptin g a 'zero trust' security architecture, a significant government initiative. They've gained access to business cloud capabilities from leading US suppliers, advancing AI, machine learning, software modernization, and cybersecurity activities. Joint Warfighting Cloud Capability contracts have been issued to tech giants such as Amazon Web Services, Google, Microsoft, and Oracle. They have optimized processes with accelerators to expedite cloud adoption, drastically lowering deployment times. The emphasis on cloud and zero trust security is part of a broader strategy to improve network security, data exchange, and workforce training, which contribute to the growth of the cloud workload protection market.

For example, in October 2022, Orca Security obtained the FedRAMP Ready certification, allowing it to deploy its agentless Cloud Security Platform to US Federal Government environments while meeting severe security criteria. Without the need for agents, the platform provides extensive insight into cloud workloads and configurations, boosting cloud security .

Impact of COVID-19

Before COVID-19, enterprises increasingly adopted cloud technologies and cybersecurity was mostly focused on traditional networks. However, the pandemic drove digital transformation and remote work, resulting in a spike in cloud usage. These moves revealed weaknesses, emphasizing the importance of robust cloud workload protection. During the pandemic, cyber risks escalated, including targeting cloud assets. As a result, there is a greater emphasis on securing cloud workloads following COVID-19, with higher investments and urgency to secure data and ensure cloud workload protection market continuity in the expanding threat landscape.

Future Market Scenario (2024-2030F)

AI and machine learning will become more important, enabling better threat

+357 96 030922
info@marketpublishers.com

detection, and automatic response methods, hence increasing the effectiveness of cloud workload protection.

As enterprises continue to move away from perimeter-based security, zero-trust security concepts will become the standard approach, guaranteeing comprehensive protection for cloud workloads.

Vendors will offer more integrated solutions that combine workload protection with other cloud security services, simplifying management and lowering organizational operational costs.

Key Players Landscape and Outlook

Key companies in the cloud workload protection market are Amazon.com, Inc., McAfee, LLC, Microsoft Corp., Check Point Software Technologies Ltd., and Broadcom, Inc. These companies are pushing cloud security solution innovation. The market outlook predicts that demand for sophisticated protection will continue to rise as enterprises expand their cloud footprints. The landscape is distinguished by the emergence of AI-driven security, zero-trust frameworks, and integrated solutions in response to rising cyber threats and demanding compliance requirements. As cloud adoption grows, these important companies will be crucial in influencing the future of cloud workload protection.

In September 2023, Check Point Software Technologies Ltd. completed its acquisition of Perimeter 81, which will enhance its SASE services with fast, secure internet access, zero trust, and rapid deployment to satisfy remote work and cloud security needs.

In July 2022, CyberArk announced many Identity Security enhancements, including automation and orchestration via Identity Flows, increased identity compliance, cloud privilege security, and secrets management. These advances are in line with the Zero Trust concept and attempt to solve the rising complexity of identity management and security.

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

7. GLOBAL CLOUD WORKLOAD PROTECTION MARKET OUTLOOK, BY REGION, 2016-2030F

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

8. MARKET MAPPING, 2022

9. MACRO ENVIRONMENT AND INDUSTRY STRUCTURE

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

17. ABOUT US & DISCLAIMER

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Cloud Workload Protection Market Assessment, By Enterprise Size [Large Enterprises, Small & Medium Enterprises], By Services [Professional Services, Managed Services], By Deployment Mode [Public Cloud, Private Cloud, Hybrid Cloud], By End-use Industry [BFSI, Healthcare, Education, Retail, Government, Others], By Region, Opportunities and Forecast, 2016-2030F

Product link: https://marketpublishers.com/r/C16AA0468FB7EN.html

Price: US$ 4,500.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/C16AA0468FB7EN.html