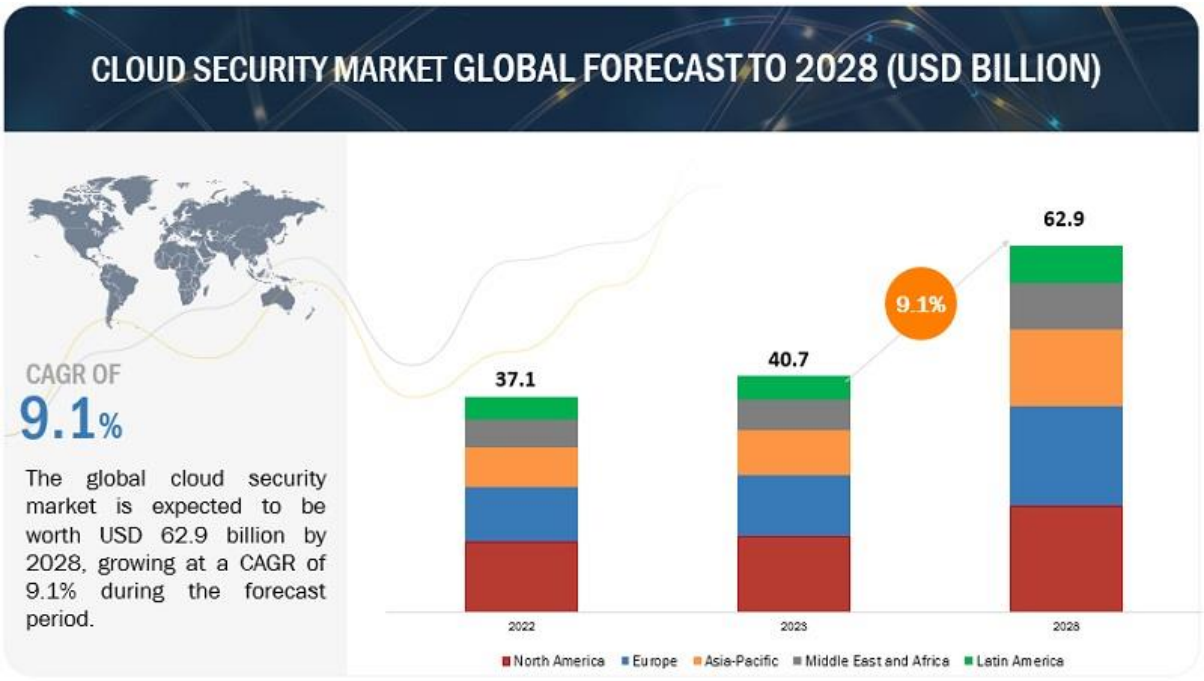
Increase in cloud services and cloud security threats

Introduction:

Over the recent past, cloud computing has moved from being a relatively new and experimental solution to being a fundamental tool for many users. This transformation is driven by the benefits cloud services offer: There are three key factors, which are considered to be important on the choice, namely scalability, cost and flexibility. Leveraging these benefits, organizations of all sizes are transitory to the cloud the storage of data and operations. However, they are valid especially when the adoption of the cloud increases as the security issues will also increase. This post discusses the cloud computing services and related security issues and risks that prevail when information is stored on the cloud resulting in the need to address the security of such information.

Cloud services: A rapidly growing market.

Market Expansion



Overall, the services provided by the cloud have and have seen a faster than exponential growth. Reported by Gartner, public cloud spending across the world is expected to tally $482 billion in 2022. Such a shift is caused by several factors, namely the evolution of hybrid and multi-cloud architectures, the development of the Internet of Things concept, and the influence of the global pandemic that accelerated Interest in remote work arrangements.

Benefits Driving Adoption

***Scalability*:** The flexibility of cloud services means that businesses put in their resources to expand the corresponding scale and vice versa. This elasticity assists in controlling costs and overheads, and ensure that an organization has the capacity to meet up with demand without having to invest in physical resources.

Cost Efficiency: This reduces capital intensive investments in IT hardware and software, as companies can rent compute cycles in the cloud. Their customers purchase only what they need in terms of consumption, and provide it through subscribes, hitherto capital intense costs to become operational costs.

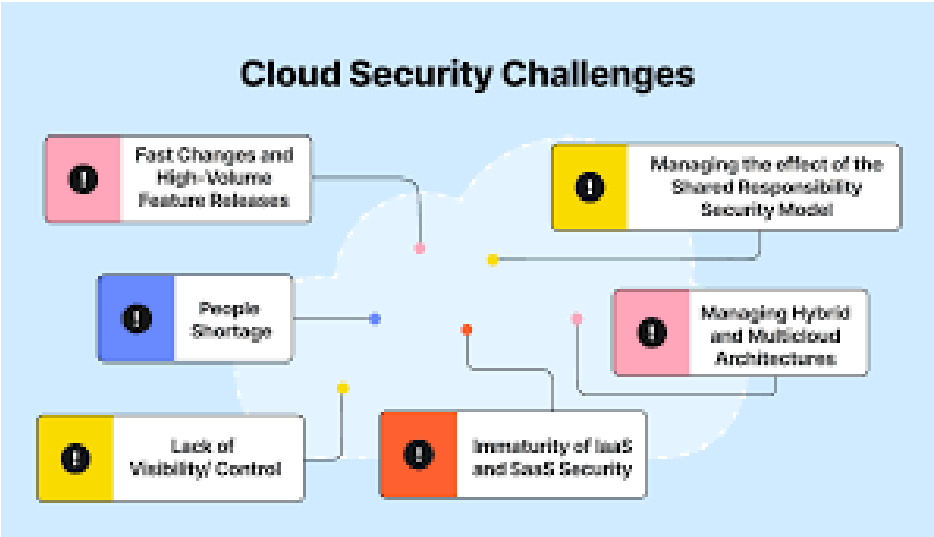
Flexibility and Accessibility: Cloud services make it possible for the employees to log into a remote server and be able to access all forms of data and applications from wherever they are, and this makes it so essential for organizations with a largely remote working team.

Disaster Recovery: Disaster recovery services in cloud environment are highly feasible since cloud providers provide great solutions for data backup and recovery in case of its loss or disruption of infrastructure.

Innovation: The cloud empowers quick and productive developmentthrough offering availabilities of different new technologies like AI, ML, and big dataanalytics for insights and growth.

The use of cloud services grows, and so do the risks While cloud adoption continues to grow, so does the threat environment. Hackers never go idle and they are always seeking new ways to capitalize on the flaws of cloud computing environments. Here are some of the most pressing cloud security threats:

1. ***Data Breaches***



Cybersecurity issues, especially in data leaks, continue to be an issue as organizations seek to adopt cloud services. Illegitimate access to confidential information can result in revenue loss and multiple fines, detrimental impact on company and product reputation, and other penalties. This is evidenced by the recent hacks of Equifax and Capital One cloud infrastructures KYRIAZIS, Accidents and breaches – Cloud computing and Storage 2017.

2. *Misconfigured Cloud Settings*

Since most organizations have implemented the cloud, misconfigurations with cloud settings are often a catalyst to security breaches. For example, setting cloud storage buckets as public or having a poor approach to IAM settings can lead to sensitive records being accessed by unauthorized personnel. In the McAfee study of common errors, it was reported that 99% of these errors were not detected and defined the importance of IaaS configuration management.

3. *Insider Threats*

External threats are equally dangerous, and the intentional or unintentional actions of a company's employees can lead to various types of dangers and risks. Organizations develop policies that control the cloud resources while giving the employees full privileges to access the cloud and hence become a target for the malicious employees who engage in unauthorized transfer of data or create an environment that is unproductive.

Account Hijacking

Account takeover is emerging as an increasingly popular attack vector where cloud accounts are targeted through mainly phishing and credential stuffing attacks. It allows them to pilfer data, install malware in the system, or abuse the availability of cloud resources to their own advantage. Overall, the risk remains high and can be managed effectively through multi-factor authentication (MFA) and proper monitoring.

5. *Advanced Persistent Threats (APTs)*

It can comprise any protracted attack in which an intruder initializes the process and remain hidden deep within the target network for a long period duration. In cloud environments, an APT attack often leads to data loss and substantial interruption of business. Adopting security measures such as; behavior analysis and threat intelligence will make it easier to detect and pullout APTs.

Insecure APIs

APIs are also crucial in cloud services, as they allow the software applications to Interface with each other. However, insecure APIs can act as points of entry for the attackers, who have a goal of disrupting operations and launching malicious activities. API is the entrance for the data to get in or out of an application and a wrong designed or no protected API results into various security threats such as data leakage, unauthorized access, etc. .

This is why cloud security should be well implemented to significantly deal with the mentioned threats. Here's why cloud security should be a top priority:Here's why cloud security should be a top priority:

Protecting Sensitive Data

Businesses have adjusted their ways of storing data and rely on the cloud, containing clients' and business' information, patents, and financial data. A breach may consequently expose the organization to severe penalties, regulatory fines, legal liabilities, and revenue loss as well as consumers' trust can be brought into jeopardy. To protect such information, efficient measures such as encryption of data, access control mechanisms, and data leakage prevention measures must be adopted.

Regulatory Compliance

Reporting to GDPR, HIPAA, CCPA, and other similar regulations is obligatory for many companies, distinguishing B2B from B2C. These regulations require organizations to implement properly secured measures of protecting their data and noncompliance leads to penalties including fines and lawsuits. Measuring cloud security is one of the steps toward compliance that must be satisfactory.

Business Continuity

Electronic crime hinders or altogether shuts businesses, implying that operations will be offline for a while and may lose sales. Preserving business operations is another advantage where proper cloud security measures ensure that the critical cloud systems do not succumb to attacks that can paralyze the cloud system. Contingency as well as backup commitments as well as adverse incident management plans are crucial to carrying on business during as well as after a security violation.

Building Customer Trust

People rely on the companies to safeguard their identity and other details they provide for commercial transactions. Confidence of customers is thus created and sustained whenever the stringently observed cloud security standards are showcased by . Analogous, the reputation of the firm is boosted. Unfortunately, the transparency of security measures and reporting of the activity where it occurs are part of the process of earning this trust.

Conclusion

An explosion of cloud services means the concept of a perimeter is gone and using perimeter controls becomes futile. A growth of new infrastructure and deployment tooling results in new environments with new security models and attack surfaces.