CLOUD SECURITY

Cloud Security

- Cloud security is a collection of procedures and technology designed to address external and internal threats to business security. Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.

- The terms digital transformation and cloud migration have been used regularly in enterprise settings over recent years. While both phrases can mean different things to different organizations, each is driven by a common denominator: the need for change.
- As enterprises embrace these concepts and move toward optimizing their operational approach, new challenges arise when balancing productivity levels and security. While more modern technologies help organizations advance capabilities outside the confines of on-premise infrastructure, transitioning primarily to cloud-based environments can have several implications if not done securely.
- Striking the right balance requires an understanding of how modern-day enterprises can benefit from the use of interconnected cloud technologies while deploying the best cloud security practices.

- In modern-day enterprises, there has been a growing transition to cloud-based environments and IaaS, Paas, or SaaS computing models. The dynamic nature of infrastructure management, especially in scaling applications and services, can bring a number of challenges to enterprises when adequately resourcing their departments. These as-a-service models give organizations the ability to offload many of the time-consuming, IT-related tasks.

- As companies continue to migrate to the cloud, understanding the security requirements for keeping data safe has become critical. While third-party cloud computing providers may take on the management of this infrastructure, the responsibility of data asset security and accountability doesn't necessarily shift along with it.
- By default, most cloud providers follow best security practices and take active steps to protect the integrity of their servers. However, organizations need to make their own considerations when protecting data, applications, and workloads running on the cloud.
- Security threats have become more advanced as the digital landscape continues to evolve. These threats explicitly target cloud computing providers due to an organization's overall lack of visibility in data access and movement. Without taking active steps to improve their cloud security, organizations can face significant governance and compliance risks when managing client information, regardless of where it is stored.
- Cloud security should be an important topic of discussion regardless of the size of your enterprise. Cloud infrastructure supports nearly all aspects of modern computing in all industries and across multiple verticals.
- However, successful cloud adoption is dependent on putting in place adequate countermeasures to defend against modern-day cyberattacks. Regardless of whether your organization operates in a public, private, or hybrid cloud environment, cloud security solutions and best practices are a necessity when ensuring business continuity.

What are some cloud security challenges?

- Lack of visibility
- It's easy to lose track of how your data is being accessed and by whom, since many cloud services are accessed outside of corporate networks and through third parties.

- Multitenancy
- Public cloud environments house multiple client infrastructures under the same umbrella, so it's possible your hosted services can get compromised by malicious attackers as collateral damage when targeting other businesses.

- Access management and shadow IT
- While enterprises may be able to successfully manage and restrict access points across on-premises systems, administering these same levels of restrictions can be challenging in cloud environments. This can be dangerous for organizations that don't deploy bring-your-own device (BYOD) policies and allow unfiltered access to cloud services from any device or geolocation.

- Compliance
- Regulatory compliance management is oftentimes a source of confusion for enterprises using public or hybrid cloud deployments. Overall accountability for data privacy and security still rests with the enterprise, and heavy reliance on third-party solutions to manage this component can lead to costly compliance issues.

- Misconfigurations
- Misconfigured assets accounted for 86% of breached records in 2019, making the inadvertent insider a key issue for cloud computing environments. Misconfigurations can include leaving default administrative passwords in place, or not creating appropriate privacy settings.

What types of cloud security solutions are available?

- Identity and access management (IAM)
- Identity and access management (IAM) tools and services allow enterprises to deploy policy-driven enforcement protocols for all users attempting to access both on-premises and cloud-based services. The core functionality of IAM is to create digital identities for all users so they can be actively monitored and restricted when necessary during all data interactions

- Data loss prevention (DLP)
- Data loss prevention (DLP) services offer a set of tools and services designed to ensure the security of regulated cloud data. DLP solutions use a combination of remediation alerts, data encryption, and other preventative measures to protect all stored data, whether at rest or in motion.

- Security information and event management (SIEM)
- Security information and event management (SIEM) provides a comprehensive security orchestration solution that automates threat monitoring, detection, and response in cloud-based environments. Using artificial intelligence (AI)-driven technologies to correlate log data across multiple platforms and digital assets, SIEM technology gives IT teams the ability to successfully apply their network security protocols while being able to quickly react to any potential threats.