Cloud benefits and limitations

You've learned that the cloud offers many benefits, especially to organizations wanting to shift away from an on-premises infrastructure. Cloud computing supports the quick, secure, and durable scaling of resources.

In this reading, you'll learn more about cloud benefits, and how they apply to the cybersecurity field. You'll also gain more perspective into the limitations of adopting cloud infrastructure. This knowledge will help you evaluate your options when deciding whether to migrate to the cloud.

Benefits

Faster time to market

One benefit of the cloud is that it has a faster time to market. Time to market is the amount of time it takes an organization to deploy software to end users. Users often have high expectations for timely software releases, and businesses want to deliver their product to meet those expectations. Using the cloud service provider's (CSP's) infrastructure enables security professionals to conduct and automate security testing from a centralized platform. The faster the software can be tested, the faster it can deploy to end users. Automating security checks also makes for a more efficient and safe development process.

Improved collaboration

The cloud makes collaboration more efficient than ever. With only an internet connection, security teams have access to shared tools hosted in the cloud. These tools enable teams to quickly identify and communicate emerging threats or vulnerabilities.

Data security

CSPs offer many security features for their users, like security controls and policies, that can strengthen their security posture. Providers like Google Cloud also encrypt data at rest and in transit, adding another layer of protection.

Durability

The cloud provides durability for your resources. Organizations using cloud data storage can configure and protect data in the event of natural disasters, equipment failures, and even in the case of malicious threats. Using a centralized cloud platform improves visibility into all of organizational resources, not just the ones stored locally.

Limitations

Shift in infrastructure control

One limitation is the shift in ownership of physical infrastructure. Organizations that have traditionally used on-premises environments have to accept the cloud provider's controls over the underlying infrastructure. Before transitioning to the cloud, it's important to understand the cloud provider's infrastructure, and how data will be stored. For example, organizations have to accept the CSP's security measures for their data centers, and all of the associated equipment that will run their services.

Security concerns

A change in who owns the infrastructure may lead to concerns about data privacy and potential attacks. This may be a major concern for some users. For example, users may be concerned about the safety of their data when they don't have physical access to where it's stored. Users may also be concerned about malicious actors accessing your remote data.

Along with learning about the CSP's infrastructure, users should also familiarize themselves with the security capabilities of their cloud provider. CSPs offer some security controls as an inherent part of using their cloud infrastructure. Users also need to consider how these specific controls will impact their resources.

Migrating existing systems

Depending on the information stored in an organization's existing systems, migrating and organizing their data to a new system and environment could be time consuming and difficult. The complexity of the infrastructure will determine the ease of the migration process. For example, the organization may need to rewrite application code to be compatible with the CSP's infrastructure. They might also need to invest time and resources to train relevant employees on using cloud tools.

Key takeaways

As a cloud security professional, it's important to understand the benefits and limitations of the cloud. Security is a key part to many of these benefits, like speeding up the delivery of applications, improving collaboration, and building a durable and secure platform. It's equally important to examine the limitations of adopting the cloud, and understand the common concerns that may come up when migrating.

During your career, you may be asked to convey security implications of cloud infrastructure to an audience that doesn't have a strong understanding of the technical aspects of security. The ability to effectively interpret and communicate this information will enable you to use your knowledge to support your organization.

Resources for more information

Review this resource for more information:

- Google Cloud’s list of the advantages and disadvantages of cloud computing