Top 5 Factors for Cloud Security Success

How secure is your cloud? It's one of the top questions IT decision-makers ask when evaluating cloud providers.[1] And as today's CIOs and CISOs explore moving increasingly sensitive workloads to the cloud, Gartner has encouraged them to apply their imagination and energy to taking advantage of the benefits of cloud-based architectures in what Gartner refers to as an "increasingly ubiquitous computing model."[2]

The truth is, today's major cloud providers often provide even better security than most enterprise data centers. In fact, Gartner predicts that through 2020, public cloud infrastructure as a service (IaaS) workloads will experience at least 60% fewer security incidents than those in traditional data centers.[3]

Ready to move to the cloud?
As you consider cloud providers, look for these 5 security must-haves:

1

Identity and Access Controls

Identity and access controls are critical to ensuring that only authorized users, groups, or applications can access internal resources. Your provider should give you access to define, enforce, and audit user permissions across services, actions, and resources.

LOOK FOR:

Seek a provider who not only grants granular access to identity solutions, but also allows you to integrate with federated logins from solutions like OAuth, SAML, LDAP, or ADFS.

2

Detective Controls

Your cloud provider should offer you the visibility you need to spot issues before they impact the business, improve your security posture, and reduce the risk profile of your environment.

LOOK FOR:

You should be able to set up automated monitoring, alerting, and robust logging. Your logs should be stored in durable storage that prevents unauthorized access.

3

Infrastructure Security Controls

The right infrastructure security controls will enable you to reduce the surface area you need to manage and increase privacy for and control of your overall cloud infrastructure.

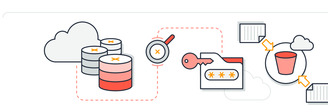
LOOK FOR:

You should have the ability to automate creation, configuration, and patching of secure OSes as well as to scale up or down depending on traffic. Make sure you have DDoS protection that can automatically close connections from dangerous sources to protect your environment from large-scale network attacks.

4

Data Protection Controls

You should have access to automatic data encryption and management services, including data management, data security, and encryption key storage.



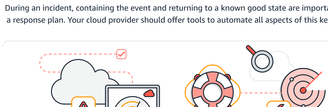
LOOK FOR:

Data encryption services should protect data in storage and databases, regardless of your database platform. We're talking about dedicated, hardware-based, cryptographic key storage. Ideally, you should also be able to discover, classify, and protect your sensitive data using machine learning and natural language processing.

5

Incident Response Controls

During an incident, containing the event and returning to a known good state are important elements of a response plan. Your cloud provider should offer tools to automate all aspects of this key best practice.



LOOK FOR:

The ability to detect changes in your cloud environment that indicate compromise, such as accessibility (IAM) changes and network or infrastructure changes, as well as the ability to automate remediation efforts. You should also be able to prepare for incidents by running your own vulnerability scans, penetration tests, disaster recovery simulations, and other critical simulated events.

READY FOR THE NEXT STEP?

Amazon Web Services

With security as our top priority, Amazon Web Services (AWS) protects millions of active customers around the world. Our customers represent diverse industries with a wide range of use cases, including large enterprises, start-ups, educational institutions, and government organizations. We depend on the same infrastructure and security services that we provide our clients, and we can help simplify meeting your own security and regulatory requirements.

To learn more, and for an expanded list of cloud security considerations, download ***Security in the Cloud: A Checklist for Cloud Buyers.***

DOWNLOAD THE CHECKLIST

REFERENCES

[1] "Diving into IT Cloud Services," *Spiceworks*, 2016. *https://www.spiceworks.com/marketing/reports/it-cloud-services/*

[2] Jay Heiser, "Clouds Are Secure: Are You Using Them Securely?" *Gartner*, September 22, 2015. *https://www.gartner.com/doc/3134527/clouds-secure-using-securely*

[3] Kasey Panetta, "Is the Cloud Secure?" *Gartner*, January 23, 2017. *http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/*