CloudCheckr

WHITEPAPER

MSP and CSP Shared Responsibility Model For Secure Customer Account Management

Executive Summary

Cloud-based Managed Service Providers (MSPs)—or Cloud Solution Providers (CSPs) with Microsoft Azure—leverage the cloud business model for reselling cloud capacity to its customers, bundled with professional services and consulting.

Many organizations lacking the experience and resources to adopt public cloud services, prefer working with an MSP or CSP and not directly with a cloud provider to make sure that their cloud deployment is well-architected, efficient and secure.

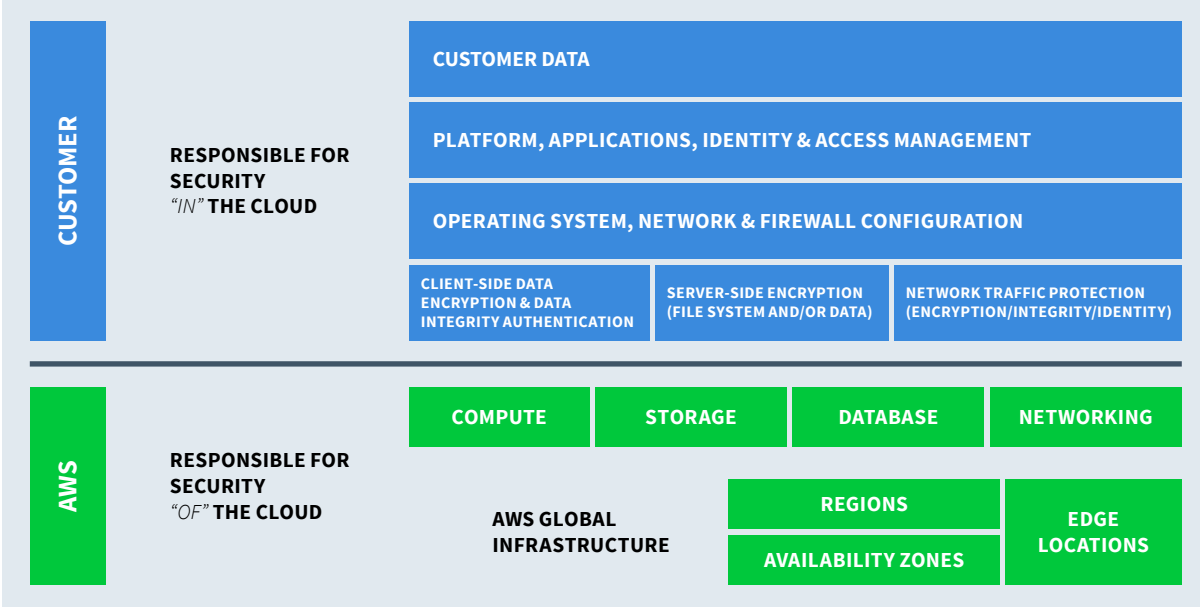
There is a cloud-related concept of shared responsibility, which refers to the distribution of responsibility for cloud security between the cloud providers and the end-users. This concept must be reexamined in cases where an MSP stands in as a mediary between them, since the responsibility is then shared by three parties instead of two.

In this paper, we will delve into the shared responsibility concept and understand the security responsibilities MSPs have towards their customers, as well as the opportunity for them to offer security as a value-added-service and revenue generator.

The Shared Responsibility Model in the Cloud

In traditional IT, all layers, from the hardware to the application, were under the control of the IT department in organizations. The public cloud, is about redirecting hardware and physical infrastructure purchase and maintenance away from the users, up to the hypervisor level, leaving the users to manage everything that sits on top of the infrastructure including OS, data and applications. This also means that the responsibility for security in the cloud becomes a shared task.

A term which was initially coined by AWS, the "shared responsibility model" is now considered a colloquial concept throughout the cloud industry, one that is used by Microsoft Azure as well as Google Cloud Platform. On a high level, it states that responsibility for designing and implementing security measures in the public cloud is neither in the sole hands of the cloud provider nor in the sole hands of the users, and discusses which party is responsible for which aspect of security. AWS refers to its responsibility as "security of the cloud", whereas the user's responsibility is referred to as "security in the cloud." While this seems like a straightforward demarcation, there are some subtleties, the main one being the type of cloud service being used: IaaS, PaaS or SaaS. In this paper we will mainly be referring to the shared responsibility with regards to IaaS.



The AWS Shared Responsibility Model. Source: AWS

Security of the Cloud

Security of the cloud, the provider's responsibility, starts at the brick-and-mortar level and extends up to the hardware and networks residing in its physical locations.

Physical Premises Security

The cloud provider is responsible for the security of its physical points of presence. This includes the provider's hyperscale data centers as well as other points of presence, for example, edge locations in the provider's CDN network. The cloud provider is responsible for perimeter security, including physical obstacles, video surveillance and patrols, as well as strict control of access to its facilities, limiting access to permitted personnel only.

In addition, the cloud provider makes sure that all supporting systems are secure and fault-tolerant. This includes maintaining high power supply and distribution, HVAC systems, and natural disaster protection. It is also responsible for failover to another physical location in case of catastrophic fault or disaster, in order to keep its customers' systems up and running.

Hosted Infrastructure

Once security of the real estate and supporting infrastructure is in place, it is also the provider's responsibility to manage security of the infrastructure itself. Compute, storage, and internal networking infrastructure (for example, networking that mounts storage volumes to compute instances) is made secure from external threats, as well as keeping customers isolated from neighboring customers in a multi-tenant architecture. To further stamp the security of their infrastructure and ensure that it can be used for various compliance and regulated workloads, the cloud providers undergo various compliance audits. In addition, they also build specialized solutions for their customers, allowing them to achieve the same compliance level on top of the cloud or build region-specific data centers to support government related workloads.

In short, the provider's security responsibility extends up to the hypervisor level, after which the customer assumes responsibility for everything else. The customer's responsibility—what is frequently referred to as security in the cloud—will be outlined in the next section.

Security in the Cloud

It only makes sense that the cloud provider assume responsibility for the security of everything under its control. Everything on top of the hypervisor level is already operated and maintained by the customer, and the customer is therefore responsible for maintaining its security.

OS, Network and Application

Once the hypervisor is installed and configured, the virtual instance is in the hands of the customers. They must assume responsibility for the security of the operating systems they install on their instances and manage OS updates and security patches, as well as the security configurations of the OS. They are also responsible for the security of the virtualized networks they deploy for communications between their resources and the outside world and all network supporting services such as firewalls, ACLs, gateways, DNS servers, DDoS protection, etc. Application security also rests in the the customers' hands as they are responsible for protecting their applications from various attacks such as SQL injections, cross-site scripting and more.

Identity and Access Management

Cloud users are responsible for configuring and managing their identity and access controls with regards to each service, virtual network, and machine.The identity and access management services are flexible enough to craft out various access control procedures, such as allowing users to only perform certain sets of actions on the resources running on the cloud. Even the visibility of resources can be controlled using various custom policies. Users can be combined into a group and later, group-based controls can be assigned, making it possible to change permissions for a set of users within the group. To make things flexible for enterprises, identity and access management services allow organizations to integrate their users using various identity providers such as SAML, which provides single sign-on capabilities.

Data Protection

Data is one of the most precious assets to any organization. When residing off customer premises and in the cloud, data can be highly susceptible to theft, takeover, and corruption. It is the customer's responsibility to secure their data, using encryption and other methods, both at rest (stored in the cloud) and in transit. Data in the cloud can be stored at the block-storage or object-storage level, and there are different data security procedures applicable for both of them.

The organization needs strong security measures not only to protect against data theft from the outside world, but also to protect against data theft from internal teams. A least-access-privileges policy should be enacted across all teams, ensuring that access to data is limited to necessary personnel only. To implement this, customers can use a combination of identity and access management policies to control access and audit logs to review events that have happened across the environment.

Where do MSPs and CSPs Fit in the Shared Responsibility Model?

Now that we have covered the shared responsibility model and where the demarcation point between the cloud providers and their users lies, let's see how it changes with an MSP or CSP in the middle.

The MSP acts as an intermediary between the cloud providers and the end-users of cloud services. It may be a reseller of cloud capacity or a managed consulting service. An MSP acting as a reseller of cloud capacity acts as a provider and bills its customers for their usage. An MSP acting as a managed consulting service has access permissions to the customer's deployment, but the customer is billed directly by the cloud provider for consumed services; the MSP charges the customer separately for value-added-services.

The responsibility for security of the cloud remains, naturally, in the hands of the cloud provider, who owns the physical infrastructure. The MSP can't control anything within the provider's physical locations and therefore relies on the provider's responsibility. Within the realm of security in the cloud, the MSP and its customer define a shared responsibility model of their own. In this case the point of demarcation is dynamic, and can change for the MSP both from customer to customer, as well as from time to time with the same customer.

It's also crucial to understand that customers can't simply hand over all responsibility of security to the MSP. To an extent, some of the responsibility will always remain in the hands of the customer. For example, even in an extreme case where the customer delegates responsibility for identity and access management to the MSP , some of that task will still be left up to the customer, e.g. users choosing secure passwords and keeping them to themselves.

On top of the role it takes in managing its customers' security, the MSP has an additional liability, which lies in the fact that it manages multiple customers. It is impossible to manually handle the security requirements and responsibilities defined with each customer, and the MSP must use a central management platform to keep track of each and every customer's security requirements, status, and access keys. It must also ensure that all customer data remains confidential and inaccessible to other customers.

The cloud providers, while technically not responsible for security in the cloud, offer numerous tools which help MSPs track and manage their customers' security, besides those offered by third parties. To name just a few:

TYPE OF SERVICE	OBJECTIVE	KNOWN AS
Logging and Monitoring	Collecting and analyzing different logs, including security, governance, and IAM logs	AWS CloudTrail and Amazon CloudWatch Azure Log Analytics Google Stackdriver Monitor
Key Management	Encryption key management	AWS KMS Azure Key Vault Google KMS
Configuration Management	Keeping inventory of all system configurations, including security configurations	AWS Config Azure Audit Logs Google Cloud Security Scanner

Summary

Cloud security is a shared responsibility of the cloud provider and its users. A cloud MSP, which steps in the middle between users and providers, takes on some of the users' security responsibility, at varying scopes, though they can never assume full responsibility for security in the cloud. They may leverage multiple services and tools offered by the cloud providers or third-party security partners to manage their customers' security requirements and ongoing operations.

An example of one of these MSPs is JHC Technology. It helps organizations in the public sector, government, and commercial spaces execute and manage their cloud transformation journeys. This includes planning, migrating, refactoring, and managing and optimizing the customer environment once in the public cloud. JHC leverages the powerful CloudCheckr platform, for speeding service delivery and mitigation of security and configurations issues of their customers among other benefits. Mike Meluso, senior cloud engineer at JHC, said that with CloudCheckr "JHC can regularly utilize insights from security reports, such as perimeter assessments or network config reports, to help our customers optimize their environment from both a cost and general efficiency standpoint."

The many disparate security services and tools, as well as the need to manage many customers' requirements, complicate MSP security management. Therefore, they must use a central cloud security management platform, one which will aggregate all security reports and alerts per customer, and provide insight into the state of security for each customer.

> **Contact us to learn more** about the role of MSPs in their customers' cloud security.

About CloudCheckr

The CloudCheckr platform offers a single pane of glass across infrastructure to ensure total security and compliance, while optimizing cost and expenses. With continuous monitoring, 450 best practice checks, and built-in automation, CloudCheckr helps organizations to ensure compliance for highly regulated industries, with alerts, monitoring, and audits to meet FedRAMP, DFARS, HIPAA, PCI, and other security standards. With deeper intelligence across cloud infrastructure and a unified cloud management solution, organizations can prevent risks and mitigate threats before they occur. Get started at cloudcheckr.com/getstarted.

VISIT US ONLINE