Shared Responsibilities

for Cloud Computing

Microsoft

Disclaimer

Published April 2017

Version 2.0

Acknowledgements

Author: Frank Simorjay

Reviewers: Alan Ross, Tom Shinder, Katie Jackson (CELA), Joel Sloss, Eric Tierling, Steve Wacker

Executive Summary

Microsoft® Azure™ provides services that can help customers meet the security, privacy, and compliance needs. This white paper helps explain the relationship between cloud service providers (CSPs) and their customers, and notes their roles and responsibilities. Standards such as National Institute of Standards and Technology (NIST) (Special Publication 500-292) and the PCI Standards Council (Information Supplement: PCI DSS Cloud Computing Guidelines) provide considerations for shared responsibilities. This paper also examines the relationships between CSPs and their customers in more detail.

In addition, this paper helps explain the shared roles and responsibilities an organization needs to consider when selecting a cloud model, such as IaaS, PaaS, and SaaS. The paper also explores the compliance requirements that need consideration based on the service model that is selected.

Table of Contents

Moving to the cloud

As organizations consider and evaluate public cloud services, it is essential to explore how different cloud service models will affect cost, ease of use, privacy, security and compliance. It is equally important that customers consider how security and compliance are managed by the cloud solution provider (CSP) who will enable a safe computing solution. In addition, many organizations that consider public cloud computing mistakenly assume that after moving to the cloud their role in securing their data shifts most security and compliance responsibilities to the CSP.

Cloud providers by design should provide security for certain elements, such as the physical infrastructure and network elements, but customers must be aware of their own responsibilities. CSPs may provide services to help protect data, but customers must also understand their role in protecting the security and privacy of their data. The best illustration of this issue involves the poor implementation of a password policy; a CSP's best security measures will be defeated if users fail to use complex or difficult-to-guess passwords.

Cloud service and delivery models

NIST defines cloud computing as a service delivery model that includes the following essential characteristics:

- On-demand self-service – users can provision services on their own
- Broad network access – service is available on any medium or device, including mobile
- Resource pooling – multiple users and dynamic access to pooled resources
- Rapid elasticity – resources can expand or contract as quickly as they are used or freed
- Measured service – services are charged based on what is used

NIST also defines three primary cloud service delivery mechanisms: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

Shared responsibilities

Microsoft understands how different cloud service models affect the ways that responsibilities are shared between CSPs and customers.

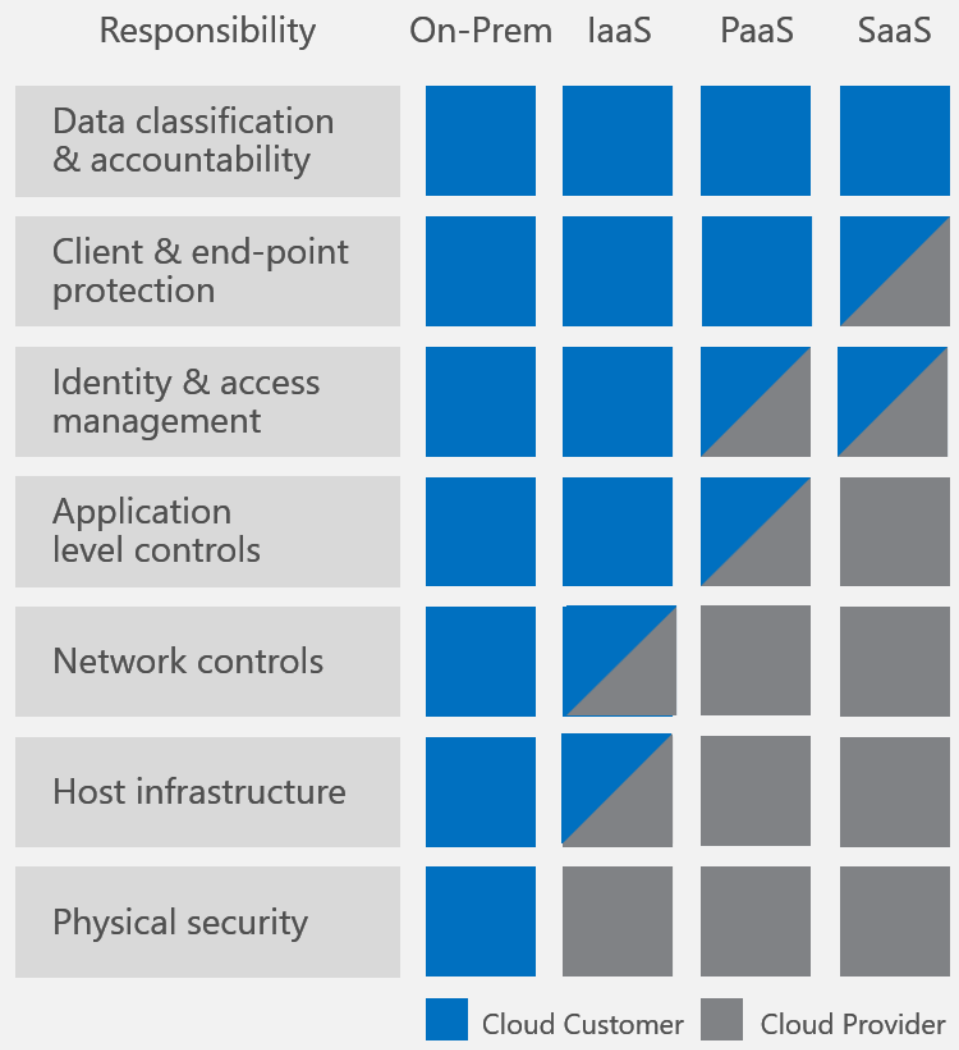

Figure 1: Shared responsabilities for different cloud service models

In Figure 1, the left-most column shows seven responsibilities (defined in the sections that follow) that organizations should consider. These responsibilities contribute to achieving a compliant and secure computing environment.

Ensuring that the data and its classification is done correctly and that the solution will be compliant with regulatory obligations is the responsibility of the customer. Physical security is the one responsibility that is wholly owned by cloud service providers when using cloud computing.

The remaining responsibilities are shared between customers and cloud service providers. Some responsibilities require the CSP and customer to manage and administer the responsibility together,

including auditing of their domains. For example, consider Identity & access management when using Azure Active Directory Services; the configuration of services such as multi-factor authentication is up to the customer, but ensuring effective functionality is the responsibility of Microsoft Azure.

Compliance obligation, data classification & accountability

In both on-premises and cloud models, the customer is accountable to ensure their solution and its data is securely identified, labeled, and correctly classified to meet any compliance obligation. Distinguishing between sensitive customer data and content designed to be public must be done by the customer. Data classification can be a complex process, but it is an important issue that all organizations considering any change, including moving to the cloud, need to consider. A data classification approach as outlined in the 'Data Classification for Cloud Computing' white paper can be used as a starting point.

SaaS solutions such as Office 365 and Dynamics 365 offer capabilities to protect customer data, such as Office Lockbox and Data Loss Prevention, but ultimately customers must manage, classify, and configure the solutions to address their unique security and compliance requirements.

For PaaS solutions, a customer's accountability for data classification and management should be acknowledged as an essential part of the planning process. In such solutions, customers need to configure and establish process to protect both the data and the solution's feature set that protects their data. Azure Rights Management services is a PaaS service that provides data protection capability for customers and is integrated into many Microsoft SaaS solutions.

With an IaaS service model, for capabilities such as virtual machines, storage, and networking, is the customer's responsibility to configure and protect the data that is stored and transmitted. When using IaaS-based solution, data classification must be considered at all layers of the solution. A misconfigured server can affect how the data that is stored in the service is protected. Compliance also requires that customers audit all deployed virtual machines within their solutions.

Client & end-point protection

As more diverse devices are used, it is also essential that clear boundaries be defined and responsibilities identified for the devices that are used to connect with a cloud service. CSPs may facilitate capabilities to manage end-point devices. For example, Microsoft Intune provides secure device management, mobile application management, and PC management capabilities. However, using a mobile management solution will still require customer accountability for their users.

Identity & access management

User or identity management is one of the core services that organizations work to provide in a seamless fashion, and in ways that are simple to use and easy to manage. Identity & access management provides users the ability to access and use resources in their environment; it is the glue between the 'who' and the 'what' shown in Figure 2.

Figure 2: Who does what

In PaaS and SaaS solutions, Identity & access management is a shared responsibility that requires an effective implementation plan that includes configuration of an identity provider, configuration of administrative services, establishing and configuration of user identities, and implementation of service access controls. Additional considerations that should be considered are the use of two-factor authentication, role-based access control, just-in-time administrative controls, and monitoring and logging of both users and control points.

Cloud solutions such as Azure Active Directory (Azure AD) provide capabilities such as multi-factor authentication, identity protection, and robust role-based access control. Azure Active Directory also provides the ability to provision on-premises and third-party applications such as Box, Concur, Google Apps, Salesforce, and more. CSPs that can provide extendible SSO capabilities can help tie together customer and CSP responsibilities with less risk of security and privacy misconfigurations.

IaaS solutions require customers to also configure and manage the identity and access controls on the managed hosts and virtual machines. Solutions such as Azure AD support identity and access management for virtual machines but must be configured at the virtual machine level. Attention must also be paid to the additional security and compliance responsibilities when running infrastructure layered services.

Application level control

Platform-managed applications and services such as web services, batch, docDb, IoT, analytics, media services, and many other related capabilities reduce customers' responsibilities by providing a more comprehensively secure solution that is managed by the CSP. Managed applications require customers to configure the services correctly, but offer more comprehensive security capabilities and integration with other solutions, such as identity management.

This shared responsibility between CSP and customer can be illustrated in a web service deployment. By default, an Azure web service is publicly open to view, which may or may not be the desired state and requires customer configuration to address the need of the solution being designed. One benefit of PaaS solutions is that they do not require the customer to implement the same security configurations as an infrastructure deployment, such as a virtual machine, by itself, since a CSP already takes care of that. Examples include patch management, antimalware, and baseline configuration. Additionally, a CSP's compliance audit reports can be used to supplement a customer deployment to meet regulatory obligations, and compliance effort.

In the IaaS service model, customers are responsible for protecting and securing the operating system and application layers of virtual machines they deploy from attacks and compromises. For example, if the IaaS deployment goal is to establish a web service offering, the administrator will need to secure the virtual machine as well as web service, which requires expertise in several security domains. The VM stack, both in Windows and in Linux, requires skilled administrators to manage and secure the host and its dependencies.

Network control

Network control includes the configuration, management, and securing of network elements such as virtual networking, load balancing, DNS, and gateways. The controls provide a means for services to communicate and interoperate.

In SaaS solutions, network controls are managed and secured for customers as part of a software as a core offering, because the network infrastructure is abstracted from them.

As in SaaS solutions, most networking control configuration in a PaaS solution is done by the service provider. With Microsoft Azure, hybrid solutions are the exception because virtual machines are placed on an Azure Virtual Network, which allows customers to configure network level services.

In an IaaS solution, the customer shares responsibility with a service provider to deploy, manage, secure, and configure the networking solutions to be implemented.

Host infrastructure

The Host infrastructure responsibility includes the configuration, management, and securing of the compute (virtual hosts, containers, service fabric, auto scaling), storage (object, CDN, file storage), and platform services. The CSP will operate and secure the host services, such as the operating systems of the service.

IaaS providers have a shared responsibility with customers to ensure that the service is optimally configured and secured. This responsibility includes the configuration of the permissions and network access controls required to ensure that networks can communicate correctly and that devices are able to attach or mount the correct storage devices.

As with Network control, host controls in an IaaS deployment require customers to be familiar with managing and securing virtual machines. This requirement includes the network management, patching, operating system configuration, application feature deployment, access control, and identity management configuration. IaaS solutions require the most understanding of the host operating system and supporting service stack

Physical security

The elements that can be considered part of Physical security include buildings or facilities, servers, and networking devices.

Customers consider the most evident value of moving services to the cloud to be the management of the physical environment. CSPs have building security processes and policies that help ensure the infrastructure is protected from unauthorized physical access, that power is maintained in a highly available method, and that if disaster strikes, the service or services should fail over to a new physical location providing continued service. Other physical security considerations are capabilities such as cooling, air management (air quality), device management, and power regulation. Microsoft follows these principles in all of its datacenters.

Conclusion

In a shared responsibility model, a layered approach to security is illustrated as:

- For on-premises solutions, the customer is both accountable and responsible for all aspects of security and operations.
- For IaaS solutions, the elements such as buildings, servers, networking hardware, and the hypervisor should be managed by the platform vendor. The customer is responsible or has a shared responsibility for securing and managing the operating system, network configuration, applications, identity, clients, and data.
- PaaS solutions build on IaaS deployments, and the provider is additionally responsible to manage and secure the network controls. The customer is still responsible or has a shared responsibility for securing and managing applications, identity, clients, and data.
- For SaaS solutions, a vendor provides the application and abstracts customers from the underlying components. Nonetheless, the customer continues to be accountable; they must ensure that data is classified correctly, and they share a responsibility to manage their users and end-point devices.

The importance of understanding this shared responsibility model is essential for customers who are moving to the cloud. Cloud providers offer considerable advantages for security and compliance efforts, but these advantages do not absolve the customer from protecting their users, applications, and service offerings.