Cloud Computing Technologies

Cloud computing is not a location but rather a pool of resources that can be rapidly provisioned in an automated, on-demand manner. The U.S. National Institute of Standards and Technology (NIST) defines cloud computing in Special Publication (SP) 800-145 as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

The value of cloud computing is the ability to pool resources to achieve economies of scale and agility. This ability to pool resources is true for private or public clouds. Instead of having many independent and often under-used servers deployed for your enterprise applications, pools of resources are aggregated, consolidated, and designed to be elastic enough to scale with the needs of your organization.

The move toward cloud computing not only brings cost and operational benefits but also technology benefits. Data and applications are easily accessed by users no matter where they reside, projects can scale easily, and consumption can be tracked effectively. Virtualization is a critical part of a cloud computing architecture that, when combined with software orchestration and management tools, allows you to integrate disparate processes so that they can be automated, easily replicated, and offered on an as-needed basis.

Cloud Service Models

NIST defines three distinct cloud computing service models:

Software as a service (SaaS). Customers are provided access to an application running on a cloud infrastructure. The application is accessible from various client devices and interfaces, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer may have access to limited user-specific application settings, and security of the customer data is still the responsibility of the customer.

Platform as a service (PaaS). Customers can deploy supported applications onto the provider’s cloud infrastructure, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over the deployed applications and limited configuration settings for the application-hosting environment. The company owns the deployed applications and data, and it is therefore responsible for the security of those applications and data.

Infrastructure as a service (IaaS). Customers can provision processing, storage, networks, and other computing resources, and deploy and run operating systems and applications. However, the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over operating systems, storage, and deployed applications, along with some networking components (for example, host firewalls). The company owns the deployed applications and data, and it is therefore responsible for the security of those applications and data.

Cloud Deployment Models

NIST also defines these four cloud computing deployment models:

Public. A cloud infrastructure that is open to use by the general public. It’s owned, managed, and operated by a third party (or parties), and it exists on the cloud provider’s premises.

Community. A cloud infrastructure that is used exclusively by a specific group of organizations.

Private. A cloud infrastructure that is used exclusively by a single organization. It may be owned, managed, and operated by the organization or a third party (or a combination of both), and it may exist on premises or off premises.

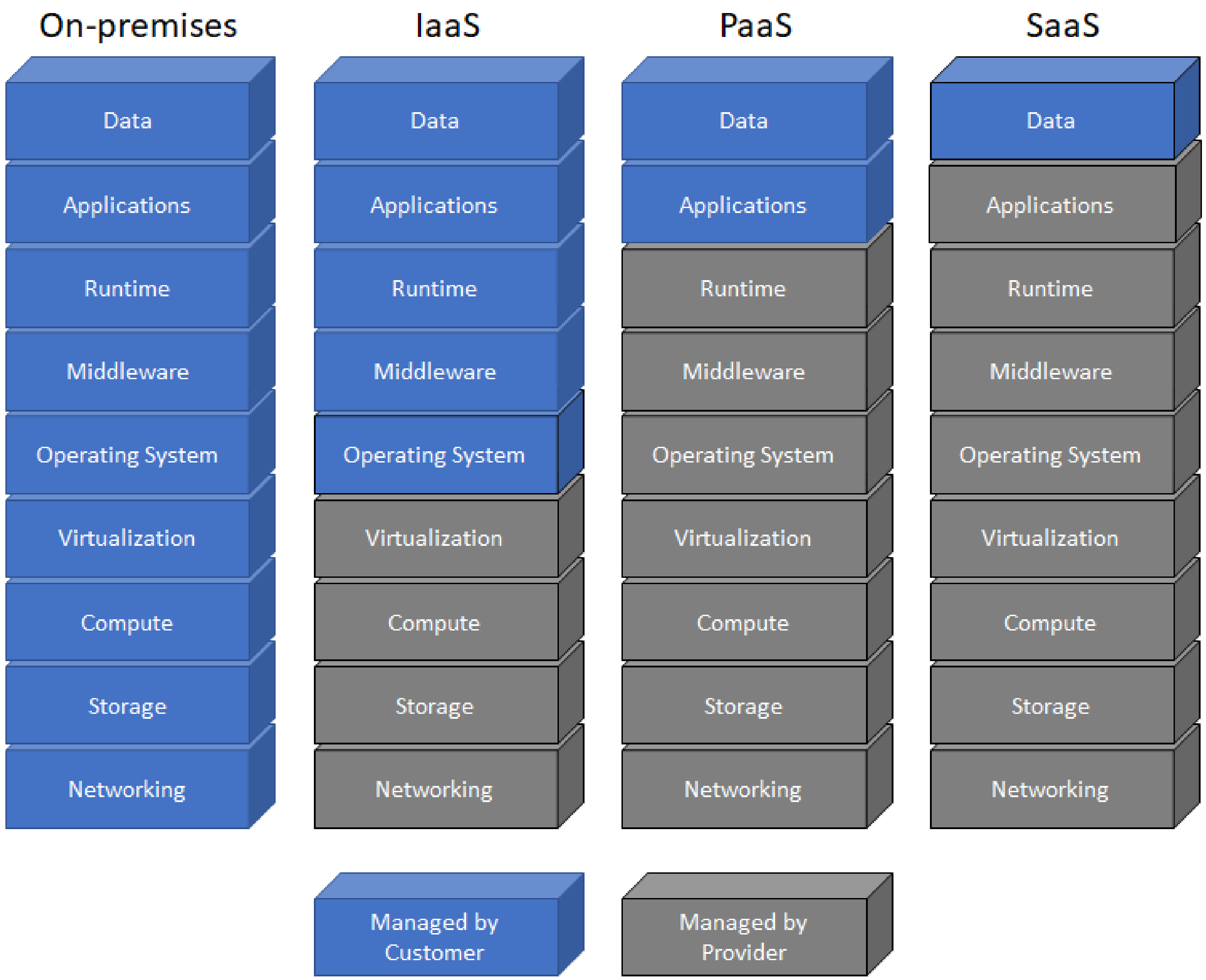
Hybrid. A cloud infrastructure that comprises two or more of the aforementioned deployment models, bound by standardized or proprietary technology that enables data and application portability (for example, fail over to a secondary data center for disaster recovery or content delivery networks across multiple clouds).

Cloud Security Challenges

The security risks that threaten your network today do not change when you move to the cloud. The *shared responsibility model* defines who (customer and/or provider) is responsible for what (related to security) in the public cloud.

In general terms, the cloud provider is responsible for security *of* the cloud, including the physical security of the cloud data centers, and foundational networking, storage, compute, and virtualization services. The cloud customer is responsible for security *in* the cloud, which is further delineated by the cloud service model (see Figure 3-1).

Figure 3-1 *The shared responsibility model*



For example, in an infrastructure-as-a-service (IaaS) model, the cloud customer is responsible for the security of the operating systems, middleware, runtime, applications, and data. In a platform-as-a-service (PaaS) model, the cloud customer is responsible for the security of the applications and data, and the cloud provider is responsible for the security of the operating systems, middleware, and runtime. In a SaaS model, the cloud customer is responsible only for the security of the data, and the cloud provider is responsible for the full stack from the physical security of the cloud data centers to the application. Multitenancy in cloud environments, particularly in SaaS models, means that customer controls and resources are necessarily limited by the cloud provider.

With the use of cloud computing technologies, your data center environment can evolve from a fixed environment where applications run on dedicated servers toward an environment that is dynamic and automated, where pools of computing resources are available to support application workloads that can be accessed anywhere, anytime, from any device.

Security remains a significant challenge when you embrace this new dynamic, cloud-computing fabric environment. Many of the principles that make cloud computing attractive are counter to network security best practices:

Cloud computing doesn't mitigate existing network security risks. The security risks that threaten your network today do not change when you move to the cloud. The shared responsibility model defines who (customer and/or provider) is responsible for what (related to security) in the public cloud. In general terms, the cloud provider is responsible for security *of* the cloud, including the physical security of the cloud data centers and foundational networking, storage, compute, and virtualization services. The cloud customer is responsible for security *in* the cloud, which is further delineated by the cloud service model. For example, in an infrastructure-as-a-service (IaaS) model, the cloud customer is responsible for the security of the operating systems, middleware, runtime, applications, and data. In a platform-as-a-service (PaaS) model, the cloud customer is responsible for the security of the applications and data, and the cloud provider is responsible for the security of the operating systems, middleware, and runtime. In a SaaS model, the cloud customer is responsible only for the security of the data, and the cloud provider is responsible for the full stack, from the physical security of the cloud data centers to the application.

Security requires isolation and segmentation; the cloud relies on shared resources. Security best practices dictate that mission-critical applications and data be isolated in secure segments on the network using the Zero Trust principle of "never trust, always verify." On a physical network, Zero Trust is relatively straightforward to accomplish using firewalls and policies based on application and user identity. In a cloud computing environment, direct communication between VMs within a server and in the data center occurs constantly, in some cases across varied levels of trust, making segmentation a difficult task. Mixed levels of trust, when combined with a lack of intra-host traffic visibility by virtualized port-based security offerings, may weaken an organization's security posture.

Security deployments are process-oriented; cloud computing environments are dynamic. The creation or modification of your cloud workloads can often be done in minutes, yet the security configuration for this workload may take hours, days, or weeks. Security delays are not intentional; they're the result of a process that is designed to maintain a strong security posture. Policy changes need to be approved, the appropriate firewalls need to be identified, and the relevant policy updates need to be determined. In contrast, the cloud is a highly dynamic environment, with workloads (and IP addresses) constantly being added, removed, and changed. The result is a disconnect between security policy and cloud workload deployments that leads to a weakened security posture. Security technologies and processes must leverage capabilities such as cloning and scripted deployments to automatically scale and take advantage of the elasticity of the cloud while maintaining a strong security posture.

Multitenancy is a key characteristic of the public cloud – and a key risk. Although public cloud providers strive to ensure isolation between their various customers, the infrastructure and resources in the public cloud are shared. Inherent risks in a shared environment include misconfigurations, inadequate or ineffective processes and controls, and the "noisy neighbor" problem (excessive network traffic, disk I/O, or processor utilization can negatively impact other customers sharing the same resource). In hybrid and multicloud environments that connect numerous public and/or private clouds, the lines become still more blurred, complexity increases, and security risks become more challenging to address.

Key Terms

Identity and access management (IAM) is a framework of business processes, policies, and technologies that facilitates the management of electronic or digital identities.

Traditional network and host security models don't work in the cloud for serverless applications. Historically, defense in depth was mostly performed through Network layer controls. Advanced threat prevention tools are able to recognize the applications that traverse the network and determine whether they should be allowed. This type of security is still very much required in cloud-native environments, but it's no longer sufficient on its own. Public cloud providers offer a rich portfolio of services, and the only way to govern and secure many of them is through *identity and access management* (IAM). IAM controls the permissions and access for users and cloud resources. IAM policies are sets of permission policies that can be attached to either users or cloud resources to authorize what they access and what they can do with what they access.

As organizations transition from a traditional data center architecture to a public, private, or hybrid cloud environment, enterprise security strategies must be adapted to support changing requirements in the cloud. Key requirements for securing the cloud include:

Consistent security in physical and virtualized form factors. The same levels of application control and threat prevention should be used to protect both your cloud computing environment and your physical network. First, you need to be able to confirm the identity of your applications, validating their identity and forcing them to use only their standard ports. You also need to be able to block the use of rogue applications while simultaneously looking for and blocking misconfigured applications. Finally, application-specific threat prevention policies should be applied to block both known and unknown malware from moving into and across your network and cloud environment.

Your business applications segmented using Zero Trust principles. To fully maximize the use of computing resources, a relatively common current practice is to mix application workload trust levels on the same compute resource. Although they are efficient in practice, mixed levels of trust introduce new security risks in the event of a compromise. Your cloud security solution needs to be able to implement security policies based on the concept of Zero Trust as a means of controlling traffic between workloads while preventing lateral movement of threats.

Centrally managed business applications; streamlined policy updates. Physical network security is still deployed in almost every organization, so it's critical to have the ability to manage both hardware and virtual form factor deployments from a centralized location using the same management infrastructure and interface. To ensure that security keeps pace with the speed of change that your workflows may exhibit, your security solution should include features that will allow you to reduce, and in some cases eliminate, the manual processes that security policy updates often require.

No matter which type of cloud service you use, the burden of securing certain types of workloads will always fall on you, never your vendor. To maximize your cloud environment security, consider the following best practices:

Review default settings. While certain settings are automatically set by the provider, some must be manually activated. It's always better to have your own set of security policies than to assume that the vendor is taking care of a particular aspect of your cloud-native security.

Adapt data storage and authentication configurations to your organization. All locations where data will be uploaded should be password protected. In addition, password expiration policies should be carefully selected to suit the needs of your organization.

Don't assume your cloud data is safe. Never assume that vendor-encrypted data is totally safe. Some vendors provide encryption services before upload, and some do not. Whichever the case, make sure to encrypt your data in transit and at rest by using your own keys.

Integrate with your cloud's data retention policy. Understanding your vendor's data retention and deletion policy is essential. It's important to have multiple copies of your data and to have a fixed data retention period. But what happens when you delete data from the cloud? Is it still accessible to the vendor? Are there other places where it might have been cached or copied? You should verify these things up front when setting up a new cloud environment.

Set appropriate privileges. Appropriate settings for privilege levels go a long way toward making your cloud environment more secure. By using role-based access controls (RBACs) for authorization, you can ensure that every person who views or works with your data has access only to the things that are absolutely necessary.

Keep cloud software up to date. Your vendor may provide infrastructure and, in some cases, a prebuilt software environment or cloud-native firewall. But anything that you add is your responsibility to secure. Thus, it's your responsibility as a user to ensure that your security patches, operating systems, and so on are up to date. The simplest way to prevent *technical debt* and backlogs is to automate the updates.

Build security policies and best practices into your cloud images. Leaving your cloud-native security to different developers on your DevOps security team might result in policy discrepancies. A good way to combat this is to create cloud images with security tools configured and policies applied so that developers can simply create instances of them.

Isolate your cloud resources. To reduce the risk of bad actors gaining complete control over your system, you should separate admin accounts for development, deployment, testing, and so on. That way, if a bad actor accesses one account, they cannot laterally

Key Terms

Technical debt is a software development concept, which has also been applied more generally to IT, in which additional future costs are anticipated for rework due to an earlier decision or course of action that was necessary for agility but was not necessarily the most optimal or appropriate decision or course of action.