Cloud Security Considerations

Cloud services are a recent model for information technology implementation and management. The cost advantages are a driving force, with security often as a secondary consideration. As with most evolving computing technologies, there are new threats to consider and address before deploying in an operational environment.

Cloud Basics

Cloud computing technology allows for on-demand, large scale, rapid deployment and configuration of computing resources. Types of cloud services include:

- Infrastructure as a Service (IaaS) – Hardware Layer
- Platform as a Service (PaaS) – Middleware Layer
- Software as a Service (SaaS) – Application Layer

Figure 1 shows the National Institute of Standards and Technology (NIST) high level cloud architectural view. This architecture is the basis for describing and relating services to an architectural framework. Security is a sub-component of the Cloud Provider.

Cloud deployments can be public, private, community, or hybrid. A public cloud is owned and managed by a third party and a private cloud is typically owned and managed internally (may be on or off-premise). A community cloud is shared by related organizations with similar requirements and a hybrid cloud is composed of two or more distinct cloud type entities coupled together.

Many organizations have hybrid deployments in which they maintain greater control of sensitive data in a private cloud. However, as cloud technology matures, public cloud security governance, compliance, and legal requirements will stabilize and make use of cloud provider standards and best practices, alleviating some of the need for hybrid implementations.

Security is a shared responsibility between the cloud provider and tenant. Ultimately it comes down to a level of trust which gets established initially by reputation and due diligence. While some trust can be mitigated through the use of technology (e.g. encryption) it is critical to understand and document the division of security responsibilities.

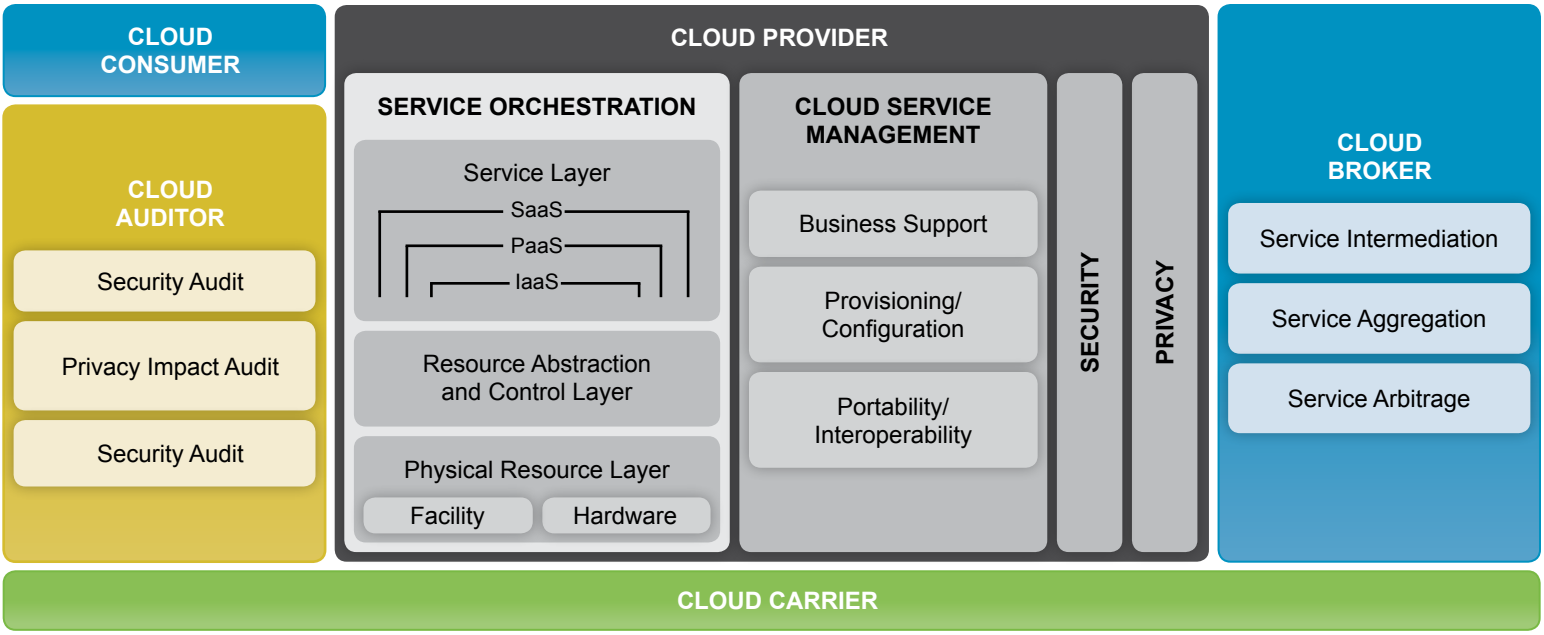

Figure 1: NIST Cloud Computing Reference Architecture

Multi-Tenancy

Multi-tenancy is the sharing of a common cloud resource that allows the cloud provider to efficiently utilize resources for multiple tenants and can be applied to all three cloud services (IaaS, PaaS, SaaS). Sharing resources, however, could result in residual data or operations being visible or discoverable by another user due to vulnerabilities or insecure configurations. There are varying degrees and definitions of Multi-tenancy among cloud providers and many providers have the option of not sharing resources at an additional cost.

API Security

Cloud providers typically have proprietary Application Programming Interfaces (APIs) that are used to build services. There are usually specific APIs for each type of cloud provider resource service, which differ in capabilities and control. Examine the type and strength of the API security features and the underlying platform to ensure that it meets or exceeds your security requirements (e.g., certificates, encryption, passwords, does not use known vulnerable configurations or platforms). The security requirements should be similar for the development and operational environments since the data is only as secure as the application accessing and modifying it.

Cloud Portability and Continuity of Operations

Develop plans and procedures to migrate and reconstitute data and services should cloud services become degraded or unavailable. Ensure that cloud data and services can be exported to a standard interchange format to provide a path for continuity of operations. Avoid being locked into a particular cloud provider. Just because data is replicated in the cloud does not mean that it can always be retrieved in a timely manner. Depending on the requirements, consider the cost-benefit of having periodic snapshots of critical and essential data securely stored outside the operational cloud so that it could be reconstituted elsewhere.

Reliability and Denial of Service

Cloud architectures are more complex and abstract than a traditional client server model. Depending on the Service Level Agreements (SLAs) with the cloud provider, various levels of service can be provided, such as redundancy, availability, load balancing, network protections, antivirus, or multiple vendors for Internet access. However, some organizations are less comfortable with managing risk in a complicated and difficult-to-understand technology like cloud, especially when they do not have direct control or access to the equipment or the operators. To enhance reliability in the case of potential cloud failures and outages, services should be redundant across different geographic regions or different cloud providers.

Cloud denial of service attacks attempt to prevent users from accessing cloud resources or services in a timely manner, by overwhelming the cloud provider's resources (e.g., network bandwidth, processor, memory, storage). Mature cloud providers employ good defenses against known attacks and quickly respond to attacks when they become aware of them.

Data Encryption

There are well established tools for encrypting data at rest and in transit, but they need to be configured and implemented properly in the cloud architecture.

Develop a robust policy to define what data needs to be protected with encryption and describe how to perform key management. Protect cryptographic keys to the fullest extent practical and change them periodically. The cryptographic keys should be managed separately for each cloud instance; they also should be managed internally or by a trusted party. Data encryption is foundational in the FedRAMP cloud requirements. Additionally, FedRAMP has hundreds of requirements that cloud providers must meet before they are considered as compliant.

Traditional Security Requirements

Figure 2 shows the typical management responsibilities for each type of cloud service. Cloud based systems still need to address traditional security requirements such as authentication, authorization, availability, confidentiality, identity, integrity, separation of duties, audit, security monitoring, risk assessment, active security defense, incident response, and security policy management. While these security requirements are not new, analyze them from the perspective of each cloud component of the NIST reference architecture even though they may be beyond your control or direct influence.

There are numerous applications to manage cloud authentication and authorization, but the capabilities and configurations need to be examined to ensure that they are compatible with your security requirements and policies.

Redeploying applications to a cloud, even a private cloud, can change the security posture. Ensure that protections provided for in the previous environment (e.g. server/host, switch, router, firewall, application firewall, logging/monitoring) are also provided for in the cloud environment.

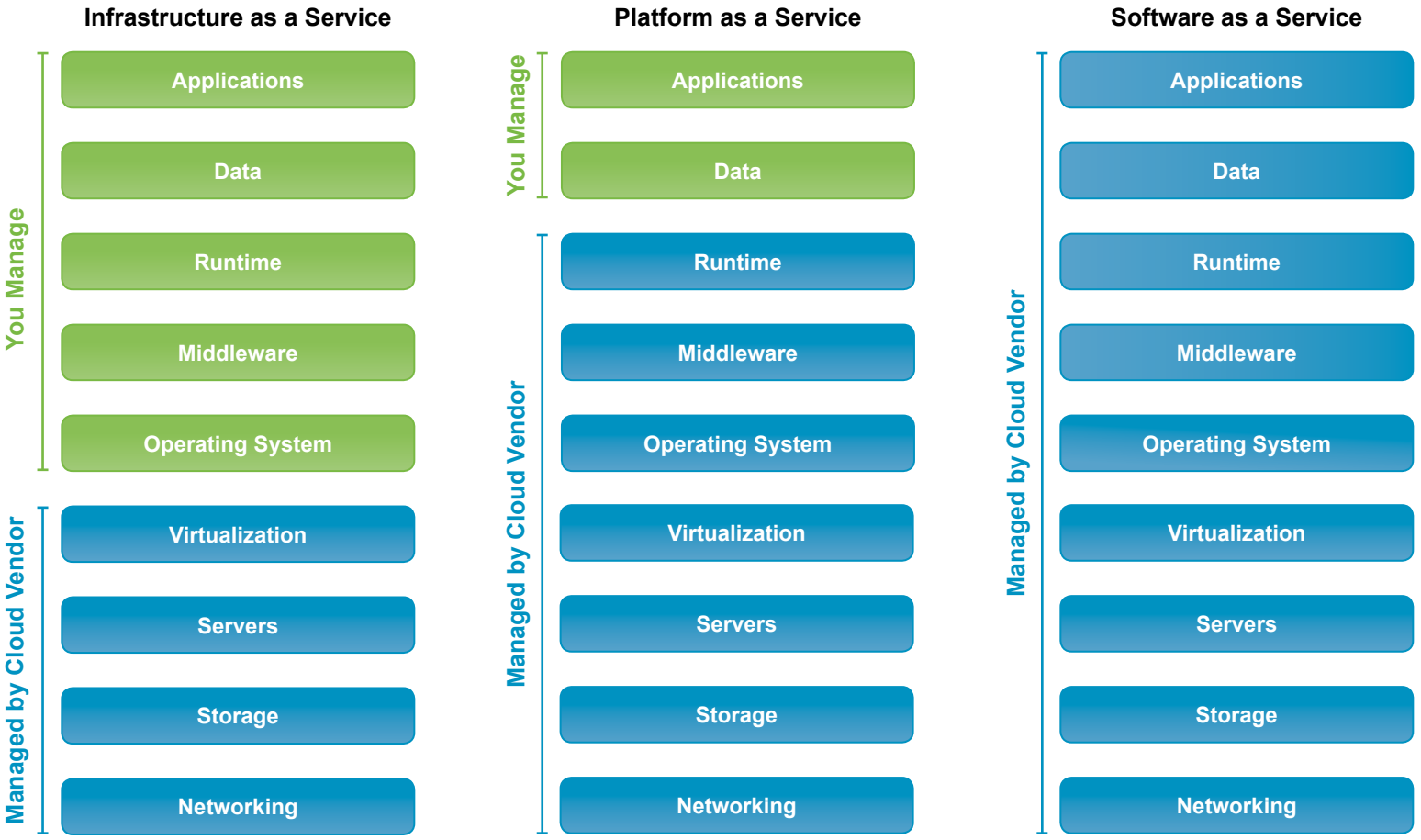

Figure 2: Cloud Management Responsibilities

Security testing should be performed periodically on cloud instances. There are open source tools, commercial tools, and companies that perform cloud security testing. Cloud providers usually require authorization and may have restrictions on what testing can be performed.

Security as a Service (SecaaS)

Many cloud providers are now offering varying degrees of Security as a Service (SecaaS). SecaaS allows the cloud customer to leverage a common set of security requirements instead of developing and deploying it themselves. The cloud provider is best postured for providing fine grain security controls since, in general, the complexity of security is much higher in a cloud environment where the data is distributed over a larger area and greater number of devices. The Cloud Security Alliance has categorized SecaaS into 10 categories and produced a document for each category.

SecaaS is becoming specialized for sectors such as medical, finance, and government, which require specific types of security protections and reporting. Determine whether SecaaS can meet some of your security or legal requirements and if it is cost effective.

Additional Information

- The Notorious Nine: Cloud Computing Top Threats in 2013
  https://cloudsecurityalliance.org
- Security as a Service Related Documents
  https://cloudsecurityalliance.org
- Cloud Computing Synopsis and Recommendations
  NIST Special Publication 800-146
  http://www.nist.gov
- Guidelines on Security and Privacy in Public Cloud Computing NIST Special Publication 800-144
  http://www.nist.gov
- US Government Cloud Computing Technology Roadmap Volume II Release 1.0 (Draft)
  NIST Special Publication 500-293
  http://www.nist.gov
- Federal Risk and Authorization Management Program
  http://fedramp.gov redirects to **gsa.gov** site
- Continuous Monitoring Strategy & Guide Version 1.1
  http://fedramp.gov redirects to **gsa.gov** site
- Additional Cloud Documents are available on a US Government restricted site
  https://www.iad.gov

Contact Information

Industry Inquiries
410-854-6091
bao@nsa.gov

USG/IC Customer Inquiries
410-854-4790

DoD/Military/COCOM Customer Inquiries
410-854-4200

General Inquiries
NSA Information Assurance Service Center
niasc@nsa.gov