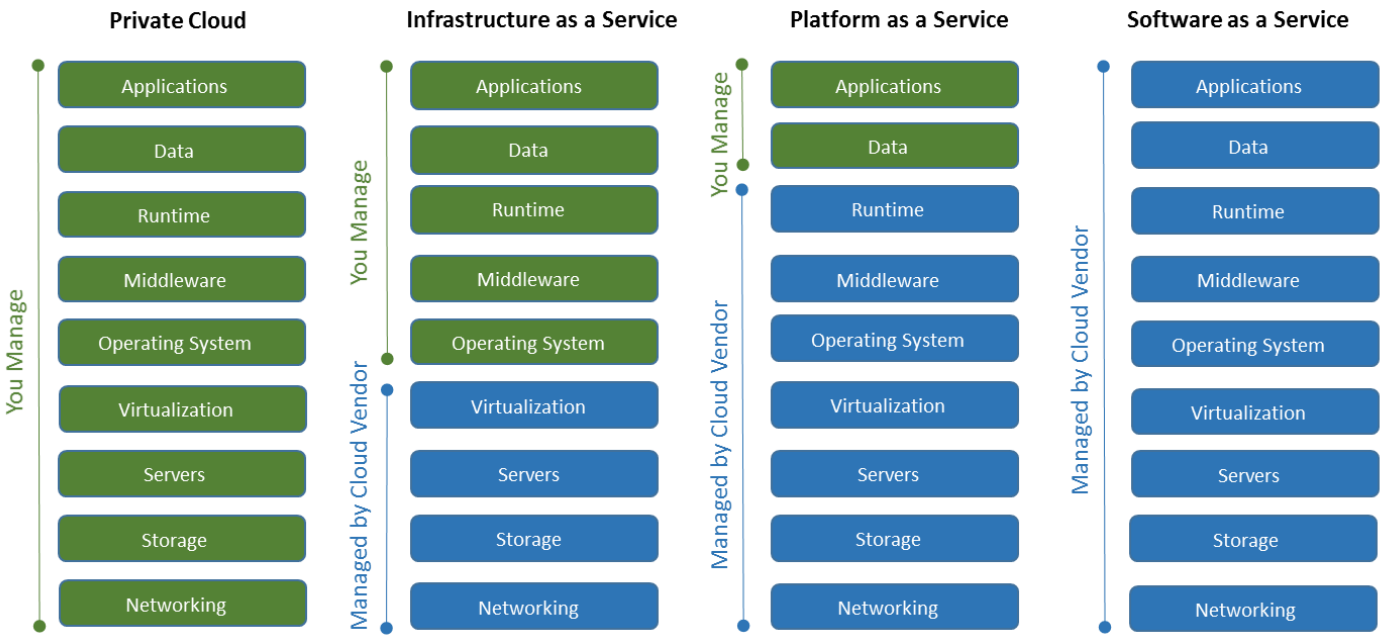
CLOUD SECURITY BASICS

BACKGROUND

Cloud services provide enterprise organizations flexibility and new capabilities, however they introduce new risks that must be understood and addressed before procuring a cloud service provider (CSP). Department of Defense (DoD) organizations are charged with handling sensitive data ranging from Personally Identifiable Information (PII) to national security information. As more sensitive data is considered for storage and manipulation in cloud environments, organizations must address new security threats before deploying in an operational environment.

INTRODUCTION TO CLOUD

Cloud services hold several distinct advantages over traditional infrastructure, allowing for rapid large-scale deployment of computing resources. Organizations have different requirements, which can be met by different types of cloud services that usually fit into three broad categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Management responsibilities (shown below) vary depending upon the type of service, and whether the cloud environment is hosted privately.



Cloud deployments can be public or private. Public clouds are owned and managed by a third-party while private clouds are usually owned and operated on-premises. Security concerns depend upon the service type as well as where the cloud service is deployed. Security should be a primary consideration when choosing a cloud service provider and deployment type. Private clouds shift more of the security responsibility to the organization. With public clouds, organizations share security responsibilities with the CSP.

Services that use the cloud to perform some functions (e.g., backup software or Personal Security Products) have the same shared responsibility and management requirements as other SaaS cloud services. Organizations should ensure that any product that uses the cloud conforms to federal and DoD requirements before deploying to their environment.

Shared Responsibility

Cloud service providers and DoD organizations share unique and overlapping responsibilities to ensure the security of services and sensitive data stored in public clouds. Typically CSPs are responsible for physical security of cloud infrastructure, as well as implementing logical controls to separate customer data. Organizational administrators are usually responsible for application level security configuration such as mandatory access controls for authorization to data. Many CSPs provide cloud security configuration tools and monitoring systems, but it is the responsibility of DoD organizations to configure the service according to their security requirements.

Threat Model

Primary risks to cloud infrastructure are malicious adversary activity and unintentional configuration flaws. Public cloud services use shared infrastructure which can lead to unintentional vulnerabilities. Foreign Intelligence Services might exploit poorly configured clouds to enable collection of sensitive DoD information. Federal law and DoD policy define how different types of sensitive data should be handled to prevent exposure. Organizations must consider what their security requirements are before making a decision on a cloud service that fits their specific threat model.

Using a public cloud service extends the trust boundary beyond the organization. New risks are introduced by utilizing CSPs, such as insider threats and a lack of control over security operations. Customers should take advantage of cloud security services to address mitigation requirements. While some threats can be mitigated entirely through the use of technical solutions (e.g., encryption), ultimately it is critical to understand and document the shared security responsibilities in order to establish trust with the CSP.

Federal and DoD Requirements

The Federal Risk and Authorization Management Program (FedRAMP)1 provides a standardized framework for assessing and authorizing cloud services. Authorized CSPs2 are vetted and certified according to a standardized set of security requirements. While FedRAMP accredits cloud service providers according to several standards, DoD organizations are still responsible for determining their requirements and whether a particular cloud service provider is authorized to handle their data.

The DoD Cloud Computing Security Requirements Guide (SRG)3 outlines the security controls and requirements requisite for utilizing cloud services within DoD. In order to be approved for use by DoD organizations, CSPs must be accredited according to requirements set by the SRG. Sensitive data should only be handled by CSPs that are accredited for that type of data. DoD mission owners must integrate SRG requirements regarding cloud security controls into their cloud architectures.

MANAGING RISK

Minimizing risk to cloud services requires careful vetting before acquisition, as well as proper configuration and continuous monitoring. Organizations should determine their threat model, ensure the chosen cloud service meets federal and DoD standards, and implement correct configuration and controls. Administrators should refer to service specific cloud security configuration guidance published by NSA. Ultimately controlling risk is a process, not a checklist. Major cloud security concerns are listed below, but specific requirements will vary.

Access Control

Misconfigured access controls in major cloud storage providers have resulted in the exposure of sensitive data to unauthorized parties. Data exposures are especially impactful for DoD as they erode public trust and in some cases can damage national security. Controlling access is a key requirement when storing sensitive data. Public cloud storage

[1] https://www.fedramp.gov

[2] https://marketplace.fedramp.gov/#/products?status=Compliant

[3] https://iase.disa.mil/cloud_security/Pages/index.aspx

providers have default access control configurations which differ from the security requirements of the information being stored. Administrators must configure permissions according to what people and systems have a need to access the data. Logging and automated systems should be used to confirm correct access control configuration. Many CSPs provide specific tooling to manage access permissions and to log unusual or unauthorized activity.

Cloud Patching

Taking advantage of software security updates is a significant part of running a secure cloud environment. The responsibility of applying software updates varies depending upon the type of cloud service used and who is responsible for its management. Updates to the underlying infrastructure will be handled by the cloud service provider. However, organizations are responsible for applying security patches to services they manage themselves in the cloud. Applying security patches as soon as they are released is critical to preventing data breaches and loss of trust.

Multi-Tenancy

Multi-tenancy allows sharing of common cloud resources between multiple collocated cloud customers. Depending upon the type of cloud service (IaaS, PaaS, SaaS), cloud service providers will allocate resources differently. CSPs at a bare minimum will implement logical controls to separate user data and operations, however vulnerabilities or unintentional configuration flaws could be exploited by a collocated malicious actor. FedRAMP and the DoD Cloud SRG define requirements for logical separation, but some organizations may require greater assurance. Private clouds or dedicated public clouds with physical separation should be used for sensitive operations as required.

Encryption

Protecting PII and other sensitive data requires encrypting data in transit as well as when stored at rest. Organizations must define a robust policy for what sensitive data should be encrypted and the process for doing so. Cryptographic keys used for encryption operations should be stored securely and separately from the cloud instance of the data being stored. Keys should be directly managed by the mission owner or by a trusted third-party. Cloud-based key management and encryption can be used for some DoD accredited clouds. FedRAMP and the DoD Cloud SRG define several requirements for encryption that CSPs must adhere to in order to be considered compliant. Depending upon the type of data being stored, organizations can encrypt sensitive data before transmitting it to a cloud service. Additionally, sensitive data should be encrypted at rest in accordance with requirements set by the DoD Cloud SRG.

Utilize Cloud Security Services

Cloud service providers are uniquely positioned to provide threat information as well as defensive countermeasures. Customers should fully take advantage of cloud security services and supplement them with on-premises tools to address gaps, implement in-house security tradecraft, or fulfill requirements for sensitive data. Trust is essential -- the risks of trusting a CSP to correctly implement security functionality must be weighed against the costs of managing security controls in-house.

Reliability and Denial of Service

Cloud denial of service (DoS) attacks prevent users from accessing cloud services by overwhelming the cloud service provider's resources. Mature CSPs will employ good defenses against known attacks and quickly respond to attacks when they are made aware of them. In order to prevent catastrophic impacts to mission, organizations must determine whether a CSP has implemented the processes and tools to mitigate DoS attacks. Whenever necessary, organizations should distribute redundant systems across multiple geographic regions or diverse cloud providers for high availability.

Data Spillage

In compliance with federal and DoD regulations, cloud service providers should only store and manipulate data they are accredited to handle. Data spillage occurs when sensitive data is unintentionally introduced into a non-accredited cloud environment. DoD organizations must have clear procedures in place to detect and remediate data spillage events.

BOTTOM LINE

Cloud services enable powerful capabilities and enterprise flexibility. However, organizations should enforce applicable security guidance and carefully determine whether their threat model fits with the mitigations offered by the accredited cloud service they are considering.

Additional Information

https://www.iad.gov

Contact Information
Client Requirements and General Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: Cybersecurity_Requests@nsa.gov