Uphold the Cloud Shared Responsibility Model

Executive summary

The threat landscape of the cloud differs from that of a traditional on-premises environment. An increasing reliance on the cloud brings new complexities and security challenges, and as a result, adversaries are increasingly targeting these environments.

Customers often incorrectly assume that the cloud service provider (CSP) manages important aspects of safeguarding resources in the cloud that are not the CSP's responsibility. CSPs provide highly automated, software-defined, and application programming interface (API)-driven platforms that "do what they're told" by customers without any human oversight on the CSP side. Misconfiguration and lack of security controls are significant risks in cloud environments.

Both the customer and the CSP are accountable for securing cloud environments. The shared responsibility model outlines the different responsibilities between the customer and the CSP. Good cloud security results from understanding those responsibilities and upholding them in partnership.

The purpose of this cybersecurity information sheet (CSI) is to educate and inform the audience regarding a security and compliance cloud framework that outlines the responsibilities of both the CSP and the customer with securing every aspect of their selected cloud instance.

Both the customer and the CSP are accountable for securing cloud environments.

Organizations should ensure that they are fully aware of their responsibilities when it comes to selecting the cloud service that best fits their needs.

Three cloud service models

Customers' responsibilities for the security of their cloud environments will differ greatly based on their choice of cloud service(s). The three main categories of cloud service models are:

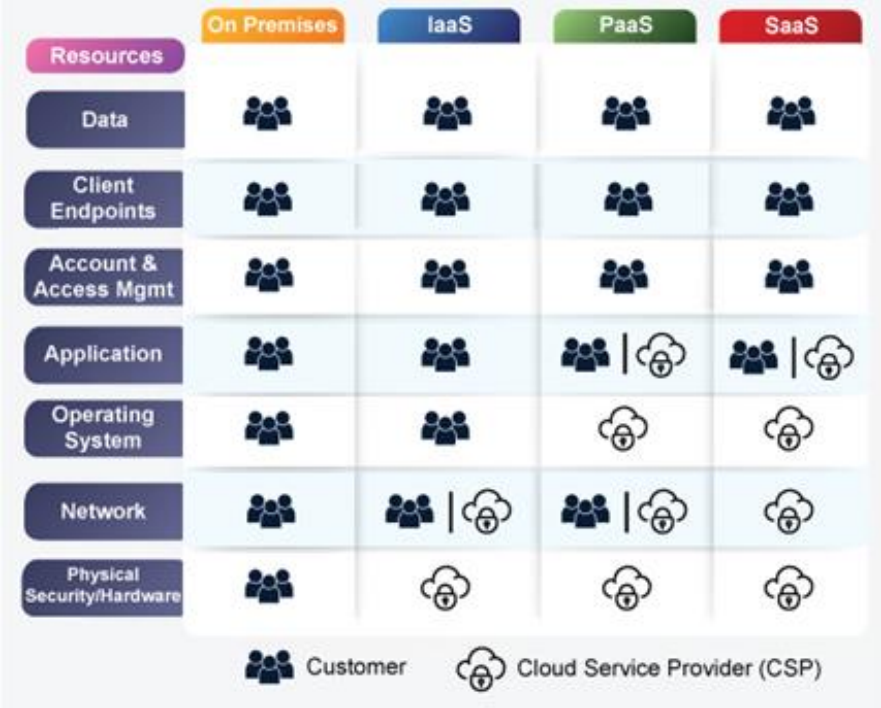
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)

- Software as a Service (SaaS)

The following figure illustrates how the responsibility is divided between the CSP and the customer for each cloud service model. While responsibilities generally follow the models identified in this CSI, specific offerings may differ. Organizations should ensure that they are fully aware of their responsibilities when it comes to selecting the cloud service that best fits their needs. [1]

When using service offerings of all model types, customers typically maintain the security of their data, endpoints, and accounts, as well as manage access control policies governing access to cloud resources in their tenant.

IaaS provides a wide range of computer infrastructure resources, such as virtualized servers, storage, and network equipment, removing the burden of on-premises infrastructure maintenance. In this model, the customer also configures network security policies and maintains the security of the operating system and applications hosted on the provided infrastructure. The CSP provisions and secures the physical resources for the customer and maintains isolation between customers.



PaaS provides customers platforms built from software, hardware, and infrastructure service subscriptions and expressed as programmable APIs that carry out work on the customer's behalf. These services are generally not similar to on-premises technologies. Software developers often leverage PaaS to eliminate managing the underlying platform. The customer's responsibilities are to configure the service properly, develop application code security, review the data used within the service, and configure security policies to

restrict network access between applications. The CSP secures and maintains the hardware, operating system, networking, and platform software configurations.

SaaS provides end-user capabilities such as email, storage, and data modeling. In this service model the customer generally configures the service, manages access control policies, and secures their data. The CSP secures and maintains the hardware, operating system, networking, and application software. SaaS offerings in particular have a wide range of security models and consequently, customer responsibilities for these services will vary.

Organizations must understand the details of their responsibilities for each offering that they use. CSP documentation and terms of service outline how the customers and CSPs share the responsibilities.

Customer accountability

Customers often assume the CSP's responsibility to protect customer data is broader than it actually is, leading to the customer failing to take needed actions. Many CSPs commit to access customer resources only under specific circumstances, and often only with consent or notification from the customer. Typically, this access is to support a customer support request.

Organizations must control access to the information in their cloud resources. Customers should identify the appropriate personnel who will be granted access and ensure that data is protected by denying access to all others. They should also ensure applications deployed in the cloud are secure by design and by default. For more information, see the NSA and CISA CSI: Use Secure Cloud Identity and Access Management Practices.

Security considerations

Cloud vendors may share security assessments by independent third-party evaluators, but customers usually cannot perform any security testing of the underlying cloud infrastructure. Organizations should consider third-party assessments and certifications when evaluating specific cloud features.

To strengthen the security of the cloud environment, customers should perform penetration tests on their cloud tenants in accordance with CSP terms of service. These tests will focus on the customer's cloud environment.

Customers with multi-cloud environments should be aware that different vendors implement security features differently. Organizations must ensure that their security posture is strong across and between platforms. Customers should routinely check their security controls as they import data into their different cloud zones. For more information, see the NSA CSI: Account for Complexities Introduced by Hybrid and Multi-Cloud Environments.

CSPs are constantly making updates to their environments. Service updates and configuration changes could potentially negatively alter service security. Processes are in place to prevent this from happening, but these processes are not necessarily foolproof.

Cyber breaches and data spillages occur, and likely occur more frequently than reported. Most CSPs publicly provide incident response guidance for customers including:

- Outlining response planning and procedures
- Recommending best practices
- Providing playbooks for common scenarios
- Giving security contact details
- Advising on how to gather and use indicators of compromise
- Instructing on finding lessons learned and how to apply them
- Guiding how to track incident metrics, such as mean time to detection, mean time to acknowledgement, meantime to containment and recovery

Best practices

To ensure all shared responsibilities are met, current and future customers should consider the following shared responsibilities:

- **Incident response**: The customer should review the CSP's incident response procedures, and put together incident response playbooks to prepare for how to handle a breach.

- **Actively Hunt for Intrusions in the Cloud**: An organization's cyber defenders should be trained on defending in the cloud and be equipped with cloud security tools integrated with the customer's resources. CSPs are not responsible for detecting when cloud resources are exploited due to a customer mistake. For more details, see the NSA CSI: Manage Cloud Logs for Effective Threat Hunting.
- **Implement a DevSecOps process**: Focus on placing security in the earliest steps in the software development lifecycle. For more information, see the NSA CSI: Enforce Secure Automated Deployment Practices through Infrastructure as Code.
- **Alignment of cloud infrastructure with mission**: Customers should conduct routine assessments and inventories to validate and understand their organizational cloud resources. Customers should also align their resources to controls and to policies and procedures that best suit their goals and responsibilities.
- **Data security**: Customers are responsible for the data stored in their cloud environment. A vigorous security strategy should be in place to protect that data. For more information, see the joint CSI: Secure Data in the Cloud.
- **Authentication:** Organizations must have processes in place for secure access using phishing-resistant multifactor authentication.
- **Configure identity access management (IAM)**: Cloud IAM services implement access controls for cloud resources, following customer defined policies. For more information, see the joint CSI: Use Secure Cloud Identity and Access Management Practices.
- **Key management**: Key management is a complex area of the shared responsibility model, with the customer's area of responsibility varying greatly by option. For more information, see the joint CSI: Use Secure Cloud Key Management Practices.
- **Service level agreement (SLA)**: Reviewing and understanding the SLA enables full transparency and clear language outlining customer and CSP responsibilities. If the SLA is unclear regarding the customer's responsibilities for securely using the service offering, contact the CSP for more information.
- **Adaptation**: The CSP and customer should maintain cyber awareness as new threats emerge and strategies for defense change over time.

Further guidance

Additional cybersecurity guidance can be found at NSA Cybersecurity Advisories & Guidance. Some papers that build on the topics discussed in this CSI include:

- Cloud Top Ten Cybersecurity Mitigation Strategies
  - Use Secure Cloud Identity and Access Management Practices
  - Use Secure Cloud Key Management Practices
  - Secure Data in the Cloud
  - Enforce Secure Automated Deployment Practices through Infrastructure as Code
  - Account for Complexities Introduced by Hybrid Cloud and Multi-Cloud Environments
  - Manage Cloud Logs for Effective Threat Hunting

For a list of cloud service models, deployment strategies, and security standards, see the NIST Cloud Computing special publications. [2] [3]

Works cited

[1] NSA. Mitigating Cloud Vulnerabilities. 2020. https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

[2] NIST. Special Publication 500-292: NIST Cloud Computing Security Reference Architecture. 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

[3] NIST. Special Publication 500-291v2: NIST Cloud Computing Standards Roadmap. 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf

Disclaimer of endorsement

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries or Customer Requests: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov