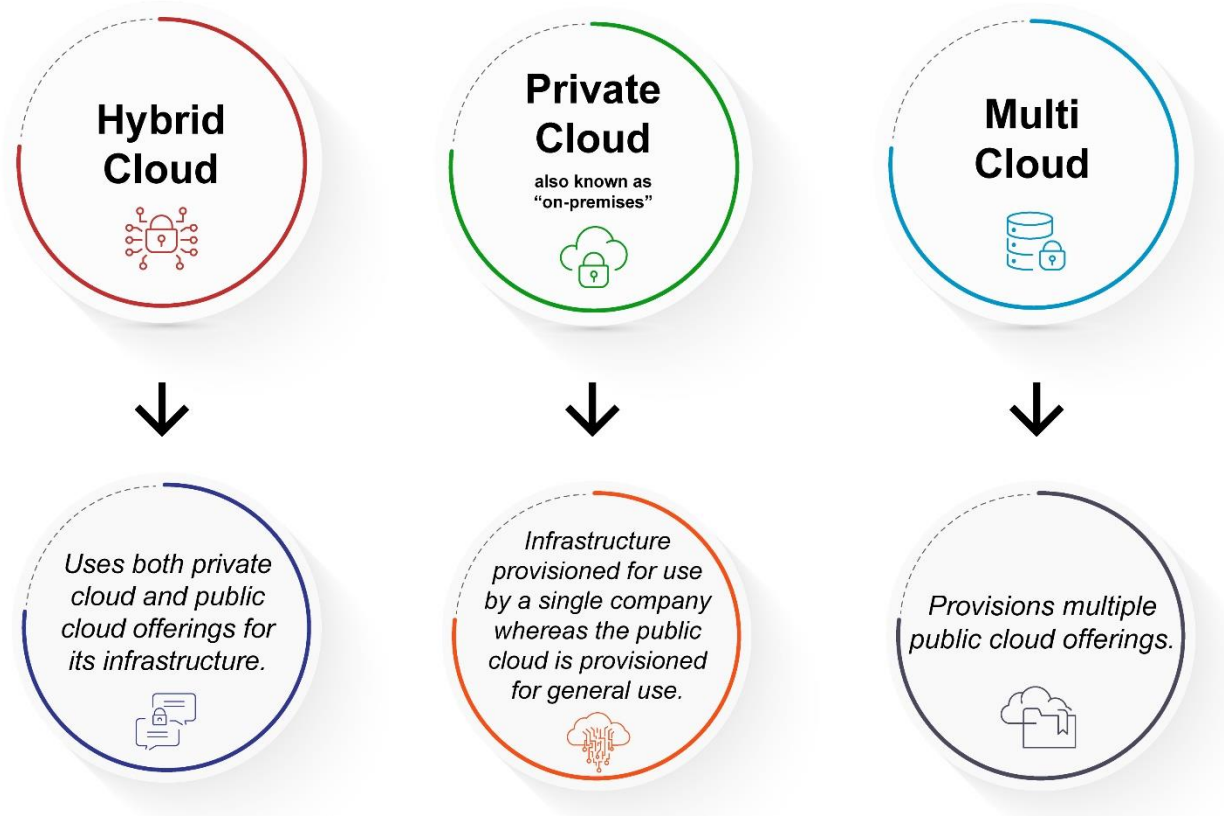
Account for Complexities Introduced by Hybrid Cloud and Multi-Cloud Environments

Executive summary

A hybrid cloud is an environment that uses both private cloud and public cloud offerings for its infrastructure. The private cloud, often referred to as an on-premises (on-prem) solution, is an infrastructure provisioned for use by a single company, whereas the public cloud is provisioned for general use by many organizations. A multi-cloud environment, on the other hand, provisions multiple offerings from different cloud service providers. Organizations often find themselves using one or both of these solutions when deploying their infrastructures to the cloud.

This cybersecurity information sheet addresses the complications that may arise when implementing hybrid cloud and multi-cloud environments due to increased complexity and solutions to mitigate them.



Addressing common complexities

Maintaining multiple cloud environments can become a burdensome task, especially for organizations new to the cloud. This includes the difficulties of:

- Learning the operations of various vendors
- Maintaining data flows between clouds
- Controlling user access
- Lacking unified visibility into cloud resources
- Maintaining compliance
- General lack of cloud security expertise. [1]

The following sections highlight these issues along with other complex tasks and associated security recommendations for IT professionals to securely address them.

Operational complexities

No two cloud environments are alike. Public cloud options tend to differ vastly, not only from private cloud infrastructures, but also from each other as well, often resulting in knowledge and skill gaps in the deployment and management process. Multi-cloud environments may also lead to operational siloes, where single teams or individuals maintain just one environment, causing configuration discrepancies between environments that may lead to exploitable security gaps. [2]

Standardizing cloud operations will resolve some operational complexities. Vendor agnostic infrastructure as code (IaC) solutions can be used to deploy hybrid cloud and multi-cloud infrastructures from a centralized location. Refer to Enforce Secure Automated Deployment Practices through Infrastructure as Code for more information on IaC best practices. Unified management solutions are also available to provide cloud administrators the ability to manage and monitor infrastructure resources from a central location. Administrators should familiarize themselves with the cloud offerings in their environment to avoid gaps in skillsets. Cloud training should be ongoing to maintain a good security posture.

Network protections

In hybrid cloud and multi-cloud environments, there are sometimes multiple data flows between the environments. A Zero Trust approach should be taken by minimizing the flows between environments, only allowing paths as defined by organizational policies,

and verifying all identities involved before allowing connection attempts. A misconfigured network can lead to data breaches across multiple cloud tenants and potentially a customer's on-prem environment as well. All network communications should use Commercial National Security Algorithm (CNSA) Suite approved algorithms. [3] Refer to Implement Network Segmentation and Encryption in Cloud Environments for additional network protection best practices.

ATT&CK® Tactic	Technique
Credential Access, Discovery	Network Sniffing [T1040]
Discovery	Network Service Discovery [T1046]
Defense Evasion	Unused/Unsupported Cloud Regions [T1535]

Identity and Access Management (IAM)

Identity and access management differs across cloud vendors and is a challenge in hybrid cloud and multi-cloud environments. Maintaining user identities in separate environments or maintaining secure interoperation between providers, while also maintaining the principle of least privilege, can be demanding.

Identity management

Identity servers are frequent targets for malicious cyber actors as they can be leveraged to retrieve user credentials that would grant access to on-prem and cloud environments. Federated identity is typically used for hybrid cloud and multi-cloud environments, granting users access to multiple accounts and domains using a common set of credentials. Account federation can be managed on-prem by organizations or through cloud-based Identity as a Service (IDaaS) solutions.

Complexities in maintaining on-prem identity solutions may force organizations to turn to IDaaS as a centralized solution. While IDaaS can be a viable option for maintaining accounts for multiple resources and makes user account activity more visible, it does require additional reliance on the vendor and can potentially serve as a single point of failure for all accounts.

When deciding on the best solution for organizations, the authentication mechanisms and how authentication information is stored and protected should be considered, following the guidelines presented in the NIST SP 800-63 series on Digital Identity Guidelines. [4] Refer to Use Secure Cloud Identity and Access Management Practices for additional identity and access management guidance.

Access management

Cloud vendors typically use a role-based access control (RBAC) or an attribute-based access control (ABAC) approach for resource access management. Vendor-specific IAM tools used for RBAC and ABAC are usually not scalable to other platforms as the resource definitions are vendor specific. Ideally, when implementing hybrid cloud and multi-cloud environments, access control policies should be uniformly defined, ensuring users have the same level of access across accounts. Maintaining consistency in the policies across multiple platforms, however, may become cumbersome logistically, causing confusion when assigning user roles and potentially causing overly permissive policies to be overlooked. Infrastructure as code (IaC) can be used to create, deploy, and maintain RBAC and ABAC policies for multiple cloud environments from a centralized location.

Whether defined using an IaC solution or through vendor-specific tools, keep in mind that vendors may handle privilege hierarchy differently, but the principle of least privilege should always be used when granting access to all cloud and on-prem environments. IAM policies should be periodically audited to check for irregularities.

ATT&CK Tactic	Technique
Resource Development	Compromise Accounts: Cloud Accounts [T1586.003]
Persistence	Account Manipulation [T1098]
Defense Evasion, Credential Access, Persistence	Modify Authentication Process [T1556]

D3FEND™ Tactic	Countermeasure
Credential Hardening	User Account Permissions [D3-UAP]
User Behavior Analysis	Local Account Monitoring [D3-LAM]

Logging and monitoring

Logging and monitoring are essential tasks for proactively tracking cyber threats and should be enabled for all environments in use. However, threat hunting and keeping track of user activity in hybrid cloud and multi-cloud environments can become difficult. This is due to lack of the skills or resources required to maintain constant visibility into multiple environments at once, especially when monitoring activity between cloud environments.

For real-time visibility, monitoring, and auditing for all environments, ingest logs into a centralized solution, such as Security Information and Event Management (SIEM) and/or Security Orchestration, Automation, and Response (SOAR) technologies. The aggregation of logs facilitates active monitoring and threat hunting from one location, giving users the ability to write queries and create alerts without needing to replicate the same activity in different environments.

These solutions are often packaged with machine learning anomaly detection that can be used to identify deviations from established behavioral patterns. Refer to Manage Cloud Logs for Effective Threat Hunting for more information on logging best practices.

D3FEND Tactic	Countermeasure
User Behavior Analysis	Local Account Monitoring [D3-LAM]

Disaster recovery

Cloud providers have their own methods of disaster recovery for internal systems that may impact the recovery objective for organizations. Multi-cloud solutions are often used to circumvent issues that may arise in disaster recovery by allowing organizations to quickly spin up backups stored in a different cloud environment. When using multi-cloud solutions for disaster recovery efforts of cloud assets, avoid vendor lock-in and have redundancy across multiple cloud environments.

Though this approach may require additional training to ensure service usage is understood across different environments, it helps ensure data is not lost if an outage or destructive event affects a CSP. Disaster recovery implementations should be regularly tested to ensure recovery expectations can be met if a real disaster occurs.

ATT&CK Tactic	Technique
Impact	Data Destruction [T1485]

D3FEND Tactic	Countermeasure
Platform Monitoring	Endpoint Health Beacon [D3-EHB]

Maintaining compliance and governance

Ensuring compliance standards are met can be difficult in hybrid cloud and multi-cloud environments. Policy as code, an IaC model, can be used to codify security and compliance best practices across cloud accounts. Using a cloud agnostic policy as code

solution will allow policies to be created as part of the existing cloud deployment operations for organizations to ensure all environments remain compliant.

Recommendations

If not done appropriately, securely deploying and maintaining hybrid cloud and multi-cloud environments can turn into a complicated task, leading to security gaps in environments. Consider implementing the following best practices to ensure cloud environments remain protected:

- Use infrastructure as code to deploy infrastructure resources from a centralized location.
- Ensure training is ongoing for all cloud environments in use to avoid gaps in skillsets.
- Minimize data flows between environments to paths necessary for day-to-day business operations.
- Ensure CNSA Suite approved algorithms are used.
- Follow NSA and NIST guidelines to determine the best IAM solution to meet organizational needs.
- Define access control policies uniformly to ensure user access is consistent across all environments.
- Use a centralized solution to aggregate logs and facilitate active monitoring and threat hunting.
- Avoid vendor lock-in and enable redundancy across multiple environments to ease disaster recovery efforts for cloud assets and resources.
- Codify security and compliance best practices through policy as code.

Further guidance

Supplementary NSA guidance on ensuring network environments are secure and defendable is available at NSA Cybersecurity Advisories & Guidance. Those of particular relevance are:

- Mitigating Cloud Vulnerabilities
- Top 10 Mitigation Strategies
- Advancing Zero Trust Maturity throughout the User Pillar
- Network Infrastructure Security Guide

- Identity and Access Management Recommended Best Practices for Administrators
- Selecting Secure Multifactor Authentication Solutions

Works cited

[1] National Institute of Standards and Technology. NIST Special Publication 800-146: Cloud Computing Synopsis and Recommendations. 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
[2] Cloud Security Alliance. Cloud Security Complexity. 2019. https://cloudsecurityalliance.org/artifacts/cloud-security-complexity
[3] National Security Agency. Announcing the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). 2022. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
[4] National Institute of Standards and Technology. NIST SP 800-63: Digital Identity Guidelines. 2023. https://pages.nist.gov/800-63-3

Disclaimer of endorsement

Trademarks

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: 443-634-0721, MediaRelations@nsa.gov