Secure Connection Requirements of Hybrid Cloud

cloud security alliance®

The permanent and official location for Hybrid Cloud Security Working Group is
https://cloudsecurityalliance.org/research/working-groups/hybrid-cloud-security

© 2021 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at https://cloudsecurityalliance.org subject to the following: (a) the draft may be used solely for your personal, informational, noncommercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Lead Authors:

Zou Feng
Narudom Roongsiriwong

Key Contributors:

David Chong
Rolando Marcelo Vallejos
Michael Roza
Geng Tao

CSA Global Staff:

Hing-Yan Lee
Claire Lehnert
Ekta Mishra
AnnMarie Ulskey

About Hybrid Cloud Security Working Group (WG)
As businesses are developing rapidly and Information Technology (IT) infrastructures constantly diversify, many cloud consumers find a single public/private cloud or traditional on-premises. The data center can no longer meet service requirements regarding costs, performance, scalability, security, resilience, regulations, and compatibility. Organizations are increasingly choosing hybrid cloud environments and services to meet their needs. Hybrid clouds take advantage of various clouds and traditional IT infrastructures and systematically benefit the users based on their service requirements. However, hybrid clouds pose different risks and thus bring on a different set of challenges to security. The WG aims to identify hybrid cloud security risks and countermeasures, helping users identify and reduce risk. Besides this, the WG also intends to provide suggestions on hybrid cloud governance, hybrid cloud threat profiles, and hybrid cloud security evaluation, guiding both users and cloud service providers to choose and deliver secure hybrid cloud solutions and promote security planning and implementation.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Table of Contents

© Copyright 2021, Cloud Security Alliance. All rights reserved.

1. Introduction

National Institute of Standards and Technology (NIST) defines the hybrid cloud infrastructure as a composition of distinct cloud infrastructures (private, community, or public) that remain unique entities. But are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).[1]

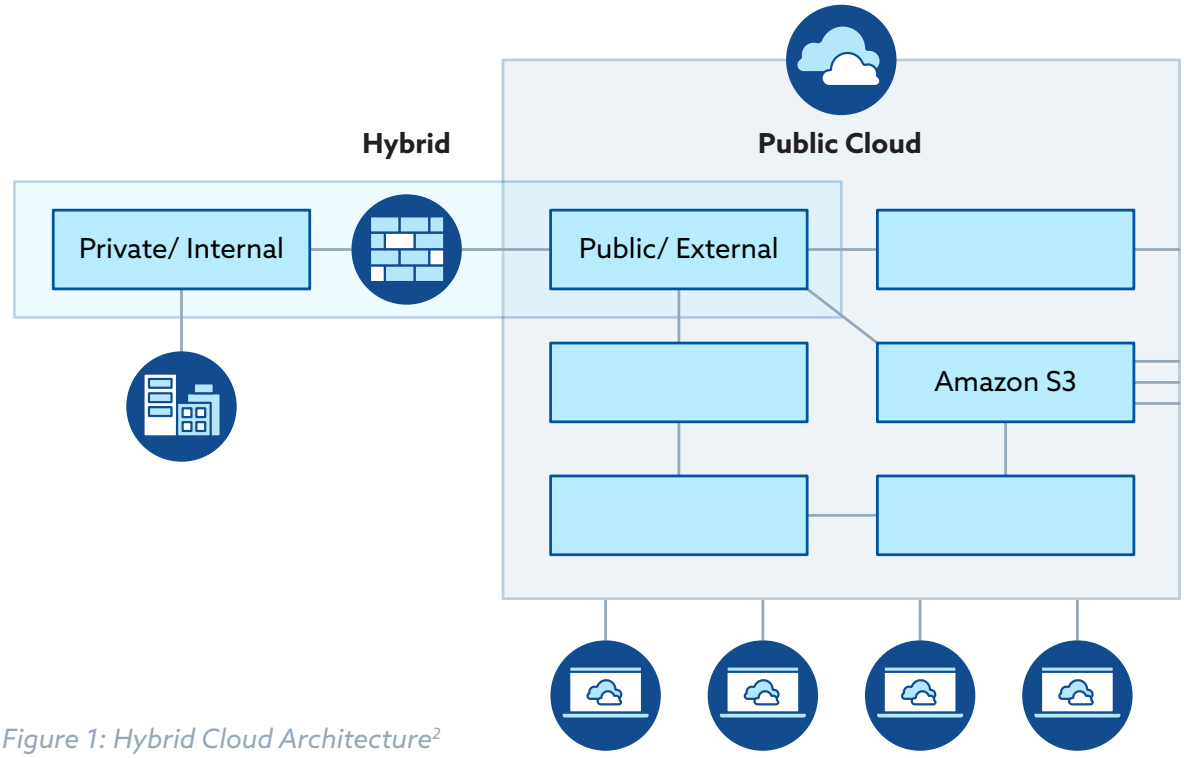


Figure 1: Hybrid Cloud Architecture[2]

Hybrid cloud environments provide enterprises with diverse resources to run different workloads depending on the Cloud Service Customer (CSC) needs. On one hand, enterprises can quickly use innovative services, deploy Internet applications, and provide optimal performance through public clouds. At the same time, the security and reliability of the private cloud can be used to run core applications in the local data center. Therefore, hybrid clouds are becoming an essential form of enterprise cloud model that allows the best of both worlds approach.

The hybrid deployment forms a diverse connected ecosystem. Data and applications flowing between clouds pose new security challenges as each cloud platform is proprietary and managed independently by Cloud Service Providers (CSPs) such as AWS, Microsoft, and Google. To successfully secure this unique and complex landscape, the enterprise should develop and employ cross-cloud security capabilities in these four areas: perimeter, transmission, storage, and management security.

This document describes the applicability of the CSA Cloud Controls Matrix (CCM) to the hybrid cloud.

[1] https://csrc.nist.gov/publications/detail/sp/800-145/final
[2] https://dzone.com/articles/5-causes-why-hybrid-cloud-is-becoming-the-new-norm

© Copyright 2021, Cloud Security Alliance. All rights reserved.

2. Cross-cloud security capabilities

Cross-cloud security consists of four elements:

1. cross-cloud perimeter security
2. cross-cloud transmission security
3. cross-cloud storage security
4. cross-cloud management security.

Cross-cloud perimeter security: Ensures the security of physical and logical boundaries between the private cloud and public cloud and cross-border access behavior, including border protection measures, cross-border access control mechanism, and interface security.

Cross-cloud transmission security: Ensures the security of cross-cloud transmissions or migration of elements such as hosts, containers, applications, and data, including network connection security, confidentiality and integrity of communication transmission, and consistency of security policies before and after transmission.

Cross-cloud storage security: Ensures the security of data storage, backup, and restoration in hybrid cloud scenarios, including storage control, encryption, and backup and restoration security.

Cross-cloud management security: Ensures security between multiple clouds through unified management, including unified identity authentication, permission management, unified Operations and Maintenance (O&M), and operational security.

2.1 Cross-cloud Perimeter Security

2.1.1 Perimeter Protection

- Set access control policies at the border between the public and private cloud to control data entering and leaving the hybrid cloud's perimeter to prevent unauthorized access.
- Set security protection mechanisms at the border between the public and private cloud to detect illegal network connections, network intrusions, and prevent malicious code.

2.1.2 Access Control

- Ensure that access from outside the perimeter is allowed only after authentication and authorization.
- Control user's permissions to cloud services that are inside the perimeter.
- Prohibit access to another user's resources (e.g. storage).
- Prohibit access to raw data (i.e., non-anonymized data under privacy protection requirements)

© Copyright 2021, Cloud Security Alliance. All rights reserved.

2.1.3 Interface Security

- Configure strict ACL rules to ensure that only applications that meet these rules can access corresponding interfaces.
- Interfaces must have access authentication mechanisms to prevent unauthorized access.
- When invoking an interface, use authentication credentials to verify the access validity.
- Interface access connections must be encrypted based on secure encryption algorithms.
- Defend against SQL injection and script injection attacks by validating interface input.
- Provide real-time and visualized interface monitoring, including the number of interface requests, interface invoking delay, and interface error information.
- Control the request frequency based on different service levels and user levels. The traffic control time unit can be seconds, minutes, hours, or days.
- Configure whitelist or blocklist of IP addresses or accounts to allow or deny access to interfaces from an IP address or an account.
- Support multiple flow control algorithms, such as leaky buckets, counters, and token buckets, to implement refined flow control in seconds.
- Support custom-traffic control policies.

2.2 Cross-cloud Transmission Security

2.2.1 Network Connection

- Deploy firewalls on the public and private cloud. Configure firewall access policies to allow only the packets that meet the specified rules. Block any other unspecified traffic by default.
- Configure virtual networks and application security groups properly and consistently across public and private clouds.
- Monitor the network traffic between the public and private cloud and report alarms immediately when exceptions are detected to prevent DoS/DDoS attacks.
- Connect private and public clouds through VPN or Direct Connect to ensure high-speed, low-latency, stability, and secure network communication.
- The service network and management network should be isolated from each other.
- Network attack behaviors, including the attack type, attack time, and attack traffic, should be recorded.
- Conduct periodic reviews to ensure that the rules remain relevant. Redundant or obsolete rules should be removed.
- Adopt well-established cryptographic algorithms and security standards.
- Consider the interoperability required to connect the different cloud platforms.

2.2.2 Communication Transmission

- Secure transmission protocols such as HTTPS and TLS should be used to encrypt channels to ensure the confidentiality and integrity of data, applications, APIs, and images during cross-cloud transmission.
- Redeploy security policies automatically when VMs, containers, applications or data migrate across clouds.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

- Support automatic deployment of security policies during cross-cloud migration of applications and data.
- Adopt well-established cryptographic algorithms and secure standards. Refrain from using custom algorithms as it may not be robust and may create interoperability issues.

2.3 Cross-cloud Storage & Compute Security

2.3.1 Data Storage

- Provide appropriate storage and encryption options based on data sensitivity and information classification. This applies at the disk, file, table storage, or database level, depending on requirements.
- The CSP should provide the CSC the capability to manage its keys used for storage encryption. Consider a Key Management System (KMS).
- Implement crypto periods to reduce the amount of data encrypted by any key and the length of time any key is at risk of disclosure.
- Store data across multiple storage volumes rather than storing data within a single data center. Use cryptographic technologies or other technical means to protect data across cloud storage to prevent unauthorized access and tampering.

2.3.2 Compute Resources

- Enable unified and consistent endpoint protection across the public and private clouds.
- Enable unified and consistent patch management across the public and private clouds for VMs and containers and other relevant components.
- Apply consistent VM and container hardening across the public and private clouds.
- Unified reporting for the above so that this can be managed by the organization effectively and holistically.
- The appropriate data at rest encryption controls should be put in place. Disk encryption is the minimum to protect the VMs.
- Consider a KMS to store and manage the keys and secrets.

2.3.3 Backup and Restore

- Establish cross-cloud business continuity and disaster recovery plans.
- Support backup protection for multiple data types, including files, emails, databases, VMs, and OSs. This can include backup of data in cloud services on Security as a Service (SaaS) / Platform as a Service (PaaS) platforms.
- The data retention requirements should be considered as part of the backup and restore approach. Distribute applications and data across multiple storage volumes to ensure rapid recovery in the most pre-incident state.
- Ensure that data is backed up from the fault point if a network or device fault occurs during the backup.
- Sync data between on-premises and cloud resources eliminating single points of failure while ensuring quick access.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

- Backups should be encrypted using strong encryption (such as 256-bit AES).
- Consider selecting hardware encryption for better backup and recovery performance.
- Use a KMS to store and manage the backup keys and secrets.
- Use the integrity check technology to verify its integrity data during backup and Disaster Recovery (DR).
- Consider Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements when selecting technology and tools needed to support efficient data recovery.
- Use cross-cloud data DR to avoid potential CSP major failure, and ensure data usability and stability.
- Train personnel and conduct DR scenarios to ensure efficiency and effectiveness of the recovery process.
- Measure the effectiveness of the DR training scenarios against the RTO and RPO objectives.

2.4 Cross-cloud Management Security

2.4.1 Identity Authentication

- Perform unified identity authentication on public and private clouds.
- Support multiple security authentication modes, such as password authentication, digital certificate authentication, and two-factor authentication.
- Administrators should set password policies of different strengths to prevent account leakage caused by simple passwords or fixed passwords for a long time.
- Enforce password complexity requirements based on corporate policies or standards. For example, the user account password should contain at least eight characters, including letters, digits, and special symbols.
- Reset lost or forgotten passwords according to policy.
- Authentication credentials (such as passwords and private keys) should be encrypted and stored using secure cryptographic algorithms.

2.4.2 Authorization Management

- Create, delete, and modify permissions for users or user groups based on role control policies.
- Support unified role control policies for public clouds and private clouds.
- Support fine-grained authorization, such as setting access control rights based on data, applications, or services.
- Accounts should be authorized based on the least privilege principle.
- The public cloud and private cloud should have the same user group permissions.

2.4.3 Key Management

- Create unified and consistent encryption management policies to govern encryption and key management across the clouds. These policies address the key management life cycle and its various phases.
- Consider using managed cloud key management services that include hardware security

© Copyright 2021, Cloud Security Alliance. All rights reserved.

modules (HSMs) and key management software. Consider its compatibility across multiple clouds.
- Carefully consider who should own the keys based on data classification, security, or compliance requirements i.e., CSP-managed keys or customer-managed keys.
- Define the roles and responsibilities clearly in terms of the parties responsible for the governance, support and usage of the keys and secrets.
- Replace keys immediately if there is good reason to suspect that the keys have been compromised or if they have reached the end of their lifecycle.
- For more details, please refer to the following publication, *Key Management in Cloud Services*[3]

2.4.4 O&M Management

- Support unified management of resources on the public and private cloud, including creating, querying, modifying, and deleting cloud resources.
- Support unified query and display of performance monitoring data on the public and private cloud.
- Support centralized alarm management, including summarizing, viewing, displaying, retaining, and exporting current alarm information.
- Configure O&M logs retention and the metrics/fields that are required to be logged.
- Obfuscate sensitive information contained in logs.
- Set log access control policies and ensure logs are tamper-proof.

2.4.5 Operations Management

- Record and analyze security events and alarms on public and private clouds.
- Support sharing and association of security events and alarms on the public and private cloud.
- Support unified management of user asset information on the public and private cloud, including physical machines, cloud host operating systems, open ports of cloud hosts, middleware, databases, web services, service applications, and cloud security devices. Ideally, a single pane of glass should be created so that the O&M teams can have full visibility across the organization's IT assets.
- Manage and deliver malicious access behaviors and code security detection policies on public and private clouds in a unified manner.
- Establish a vulnerability management framework to manage security vulnerabilities effectively based on a risk-based approach.
- This includes identifying, assessing, classifying, and remediating the security vulnerability information on public and private clouds within the established time frames.
- Build a centralized threat intelligence capability so that this knowledge can be applied comprehensively to protect information and assets.
- Consider security automation and playbooks to improve overall O&M productivity and efficiency so that the teams can focus on higher-value tasks.
- Provide a unified metering query interface to ensure that each user or functional unit can query only their information to protect user and data privacy.

[3] https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/

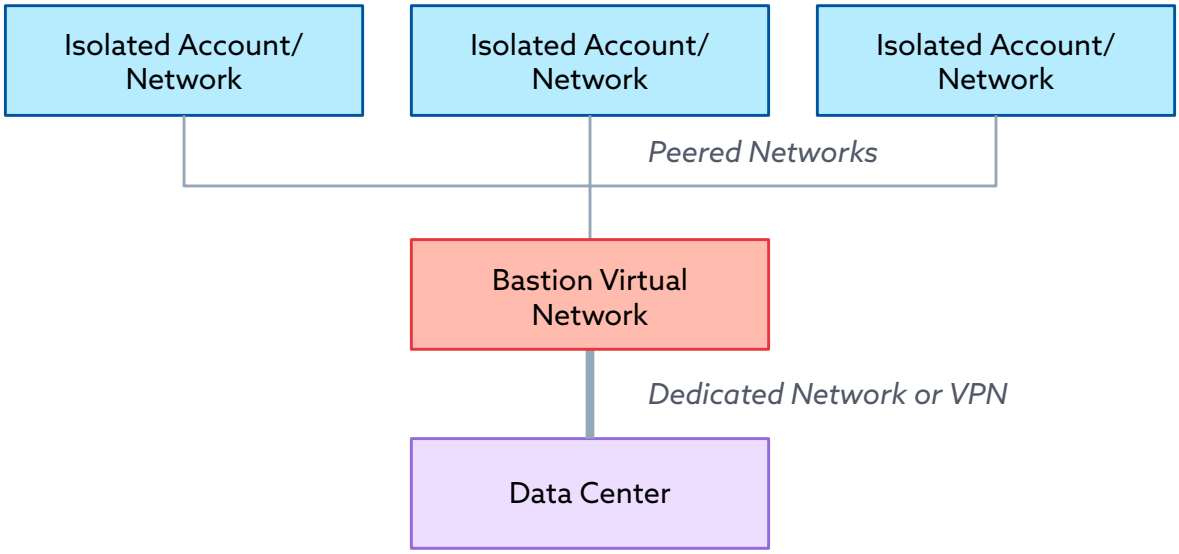
© Copyright 2021, Cloud Security Alliance. All rights reserved.

3. Practice of Secure Connection

3.1 Bastion Virtual Network

The Cloud Security Alliance's, *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*, states that "a hybrid connection shouldn't effectively flatten the security of both networks". Separation should be enforced via routing, access controls, and even firewalls or additional network security tools between the two networks. An architecture for hybrid cloud connectivity is "bastion" or "transit" virtual networks:

> - It connects multiple, different cloud networks to a data center using a single hybrid connection. The cloud administrator builds a dedicated virtual network for the hybrid connection and then peers any other networks through the designated bastion network.
> - Second-level networks connect to the data center through the bastion network, and they can't talk to each other and are segregated. Also, you can deploy different security tools, firewall rulesets, and Access Control Lists in the bastion network to further protect traffic in and out of the hybrid connection.



4.CCM Applicability

The Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing aligned with CSA best practices; and is considered the de-facto standard for cloud security and privacy. Version 4 of the CCM constitutes a significant upgrade to the previous version (v3.0.1) by delivering a substantial increase in requirements due to developing additional controls and updating existing ones.

The cross-cloud security capabilities covered by this document can refer to the related controls in the CCM v.4 control domain for implementation as below:

© Copyright 2021, Cloud Security Alliance. All rights reserved.

- cross-cloud perimeter security: Application and Interface Security (AIS), Cryptography, Encryption & Key Management (CEK) ; Threat & Vulnerability Management (TVM).
- cross-cloud transmission security: Cryptography, Encryption & Key Management (CEK); Interoperability & Portability (IPY); Datacenter Security (DCS).
- cross-cloud storage security: Infrastructure & Virtualization Security (IVS); Business Continuity Management & Operational Resilience (BCR).
- cross-cloud management security, Identity & Access Management (IAM); Logging and Monitoring (LOG); Security Incident Management, E-Discovery, & Cloud Forensics (SEF).

Reference

Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, July 2017, available @ https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Cloud Security Alliance, Cloud Controls Matrix v4.0, 2021, June 2021, available @ https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

Cloud Security Alliance, Cloud Controls Matrix v3.01, August 2019, available @ https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Cloud Security Alliance, Key Management in Cloud Services, November 2020, available @ https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/

NIST, SP 800-145, The NIST Definition of Cloud Computing, September 2011, available @ https://csrc.nist.gov/publications/detail/sp/800-145/final

ISO/IEC, 17788:2014, Information technology — Cloud computing — Overview and vocabulary, 2021, available @ https://www.iso.org/standard/60544.html

Glossary

Bastion - Platform that provides secure Remote Desktop Protocol (RDP) and Secure Shell (SSH) connectivity to all of the VMs in the virtual network in which it is provisioned. https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

Cross-cloud capabilities - unified data management platform that facilitates secure data sharing should carry out cross-cloud management. The platform gives the organization a single source of truth by allowing data to move freely across clouds. Cross-cloud compatibility drives operational efficiency in the multi-cloud.
https://www.cloudbolt.io/blog/driving-operational-efficiency-in-multi-cloud-with-cross-cloud-management/

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Acronyms

ACL	Access-Control List
AES	Advanced Encryption Standard
CCM	Cloud Controls Matrix
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
DoS	Denial of Service
DR	Disaster Recovery
EU	European Union
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IP	Internet Protocol
ISO/ IEC	International Organization for Standardization/ International Electrotechnical Commission
NIST	National Institute of Science and Technology
O&M	Operations and Management
OS	Operating Systems
PaaS	Platform as a Service
RDP	Remote Desktop Protocol
RPO	Recovery Point Objective
RTO	Recovery Time Objective
TLS	Transport Layer Security
SaaS	Software as a Service
SDP	Software-Defined Perimeter
SQL	Structured Query Language
SSH	Secure Shell
VM	Virtual Machine
VPN	Virtual Private Network
ZTNA	Zero Trust Network Access

© Copyright 2021, Cloud Security Alliance. All rights reserved.

ANNEX 1- Cloud Deployment Models

NIST Definitions:[4]

NIST Private Cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off-premises.

NIST Community Cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off-premises.

NIST Public Cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

NIST Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

ISO Definitions:[5]

Public cloud: Cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider. A public cloud may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud service provider. Actual availability for specific cloud service customers may be subject to jurisdictional regulations. Public clouds have very broad boundaries, where cloud service customer access to public cloud services has few, if any, restrictions;

Private cloud: Cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer. A private cloud may be owned, managed, and operated by the organization itself or a third party and may exist on-premises or off-premises. The cloud service customer may also authorize access to other parties for its benefit. Private clouds seek to set a narrowly controlled boundary around the private cloud based on limiting the customers to a single organization; –

Community cloud: Cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this

[4] https://csrc.nist.gov/publications/detail/sp/800-145/final
[5] https://www.iso.org/standard/60544.html

© Copyright 2021, Cloud Security Alliance. All rights reserved.

collection. A community cloud may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off-premises. Community clouds limit participation to a group of cloud service customers who have a shared set of concerns, in contrast to the openness of public clouds, while community clouds have broader participation than private clouds. These shared concerns include, but are not limited to, mission, information security requirements, policy, and compliance considerations.

Hybrid cloud: Cloud deployment model using at least two different cloud deployment models. The deployments involved remain unique entities but are bound together by appropriate technology that enables interoperability, data portability, and application portability. A hybrid cloud may be owned, managed, and operated by the organization itself or a third party and may exist on-premises or off-premises. Hybrid clouds represent situations where interactions between two different deployments may be needed but remain linked via appropriate technologies. As such, the boundaries set by a hybrid cloud reflect its two base deployments.

© Copyright 2021, Cloud Security Alliance. All rights reserved.