

ITU-T Technical Report

(06/2026)

XSTR.fcns

**Framework for cloud-native-based security
collaboration mechanism among cloud service
providers**

Framework for cloud-native-based security collaboration mechanism among cloud service providers

Summary

With the continuous development of cloud computing technology, simple private cloud or public cloud can no longer meet the demands of enterprise development, and it has become a new trend to use multi-cloud or hybrid cloud to obtain more flexible computing resources. Cloud service customers benefit from cloud services provided by multiple cloud service providers. However, this also brings numerous security challenges and poses potential security threats to cloud service customers.

This Technical Report summarizes seven security challenges in multi-cloud and hybrid cloud environments, and proposes a cloud service security framework, which mainly includes three aspects: unified security management, security collaboration and flexible security functions. Only when all parties involved in this security collaboration mechanism work closely together can they achieve strong security protection in complex and ever-changing cloud environments.

Keywords

Hybrid cloud, multi-cloud, security.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

© ITU 2026

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Technical Report	1
4	Abbreviations and acronyms	1
5	Convention.....	2
6	Overview.....	2
7	Security challenges to cloud with multiple cloud service providers	2
	7.1 Lack of comprehensive security visibility	3
	7.2 Inefficient security response coordination.....	3
	7.3 Inability to Adapt Security Policies in Heterogeneous Cloud Environments.....	4
	7.4 Security information and event management complexity	4
	7.5 Fragmented identity and access management	5
	7.6 Challenges in ensuring data security and privacy compliance	5
	7.7 Lack of secure and seamless interoperability	6
8	Framework for cloud native based security collaboration mechanism	6
	8.1 Unified security management.....	7
	8.2 Collaboration on security solutions	10
	8.3 Flexible security features.....	12
	Bibliography.....	16

Technical Report ITU-T XSTR.fcnc

Framework for cloud-native-based security collaboration mechanism among cloud service providers

1 Scope

This Technical Report analyses security challenges in multi-cloud and hybrid cloud environments involving multiple cloud service providers and introduces a cloud-native-based security collaboration framework to support coordinated security management, security information exchange and interoperable security response across such environments.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 multi-cloud [b-ITU-T Y.3537]: Use of cloud services in the public cloud from two or more independent cloud service providers at the same time for business.

NOTE – Multi-cloud, known as multi-cloud computing, is distinguished from multiple cloud which is an environment involving two or more cloud service providers (CSPs).

3.1.2 hybrid cloud [b-ITU-T Y.3500]: Cloud deployment model using at least two different cloud deployment models.

3.1.3 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.4 cloud native [b-ITU-T Y.3532]: A methodology of creating software, which takes full advantage of capabilities of cloud computing during the process of software design, development, deployment, running and management.

3.1.5 cloud service [b-ITU-T Y.3527]: One or more capabilities offered via cloud computing invoked using a defined interface. It may comprise the hardware and hypervisor layers delivering individual servers, border routers, firewalls, load balancers & switches.

NOTE – Expanded version of definition in [b-ITU-T Y.3500].

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

ABAC	Attribute-Based Access Control
API	Application Programming Interface
CI/CD	Continuous Integration/Continuous Delivery
CSC	Cloud Service Customer
CSP	Cloud Service Provider

CVE	Common Vulnerabilities and Exposures
ECS	Elastic Compute Service
HMAC	Hash-based Message Authentication Code
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
PaaS	Platform as a Service
RBAC	Role-Based Access Control
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response

5 Convention

None.

6 Overview

With the continuous development of cloud computing technology, the use of a single private cloud or public cloud may no longer meet enterprise requirements for flexible and resilient computing resources. It has therefore become common for cloud service customers (CSCs) to use multi-cloud or hybrid cloud environments involving multiple cloud service providers (CSPs). While such environments provide operational flexibility, they also introduce security challenges, including limited cross-cloud visibility, fragmented security response, evolving policy requirements and interoperability constraints.

As more industries adopt multi-cloud or hybrid cloud infrastructures, enterprises are at risk of data loss, unauthorized access, lack of visibility and non-compliance. A flexible and agile security collaboration mechanism can help enterprises improve network reliability, reduce costs, achieve centralized management and better protect their cloud assets after shielding the problems caused by heterogeneity between multiple CSPs.

Cloud-native is a methodology for creating software that takes full advantage of cloud computing capabilities during software design, development, deployment, operation and management. Cloud-native technologies support scalable, portable and resilient applications and can provide technical means for embedding security capabilities into distributed cloud environments.

Cloud-native technologies enable organizations to build and run scalable applications in modern, dynamic environments such as public, private and hybrid clouds, with the inherent potential to embed security capabilities into cloud environments and collaborate security functions across multiple CSPs. These technologies enable loosely coupled systems that are resilient, manageable and observable. By using a cloud-native approach, customers can decompose functionality into smaller, independent microservices. This makes cloud-native applications more agile because customers can immediately set up, deploy or replicate microservices with minimal compute resources. Under the cloud-native-based security collaboration mechanism, customers can inherently embed the various security functions they need into the cloud through cloud-native technologies and integrate their execution to execute predetermined security activities accordingly to meet heterogeneous cloud security needs. In this way, cloud-native, secure collaboration benefits from the agility and inherent nature of cloud-native in clouds with multiple CSPs.

7 Security challenges to cloud with multiple cloud service providers

While CSCs benefit from cloud services provided by multiple CSPs, they also face security challenges. These challenges include lack of comprehensive security visibility, inefficient security response coordination, inability to adapt security policies in heterogeneous cloud environments, complexity of security information and event management, fragmented identity and access management, challenges in ensuring data security and privacy compliance, and lack of secure and seamless interoperability.

7.1 Lack of comprehensive security visibility

In multi-cloud and hybrid cloud environments, CSCs often encounter challenges in achieving comprehensive security visibility. Security visibility refers to the ability of organizations to fully understand and monitor the security posture of their networks, systems, and applications, and is critical to identifying, assessing and managing potential security threats. Due to the heterogeneous nature of CSPs, each typically offers visibility and control limited to its own infrastructure. Security tools, access control models, logging mechanisms and monitoring interfaces are often designed for proprietary environments and lack interoperability.

Each CSP typically only provides visibility into and control over its own systems, and the account management and data protection measures they design are usually only applicable to their own platforms. This leads to complex and inconsistent protection tools and processes in multi-cloud environments, increasing the risk of schema incompatibility and potential rule loopholes. In multi-cloud and hybrid cloud environments, data is inevitably stored across different CSPs, making data monitoring and analysis more complex for enterprise cybersecurity personnel.

Second, it is natural that different cloud platforms expose heterogeneous native APIs and interfaces. However, in the absence of a unified abstraction, mediation or orchestration layer, enterprises are required to invest additional effort to integrate and coordinate interactions across multiple provider-specific interfaces. This increases the technical complexity of cross-cloud security operations and the associated management costs.

Due to the different security solutions adopted by each CSP, enterprises find it difficult to achieve a unified security view, creating security blind spots that affect overall security. Compliance management also becomes more complex, as it requires ensuring that operations across multiple cloud environments comply with local regulations and integrating data from various environments.

In summary, the absence of a unified, comprehensive security view across multiple CSPs hinders effective threat monitoring and response, making it imperative to establish a security collaboration mechanism. Enterprises using multi-cloud systems need to address the challenge of lack of comprehensive security visibility in multi-cloud and hybrid cloud environments by adopting advanced technologies and tools and developing a comprehensive security strategy.

7.2 Inefficient security response coordination

In multi-cloud and hybrid cloud environments, the ability to promptly detect, analyse and respond to security incidents is significantly hindered by architectural and operational fragmentation. Each CSP maintains its own security tools, monitoring systems and communication protocols, resulting in a lack of interoperability and consistency across platforms.

When a security incident occurs, an effective response requires timely coordination among multiple security functions, including threat detection, alerting, incident triage and remediation. However, the heterogeneity of CSP security ecosystems creates barriers to such coordination. Variations in logging formats, incident severity classification and data access interfaces prolong incident investigation and hinder automated response capabilities.

Furthermore, distributed deployment of applications and services across CSPs leads to dispersed resources, inconsistent security policies and limited centralized management. This complicates

visibility into interdependent systems and increases the likelihood of security incidents propagating across platforms. In some cases, security risks are exacerbated when enterprises prioritize business continuity by selectively bypassing certain inspection or protection mechanisms due to performance constraints, such as high volumes of encrypted data or resource-intensive services.

Improving the efficiency of security response often requires the help of automated security tools that automatically help the system make decisions. In a multi-cloud environment, this becomes cumbersome when the billions of applications running and connected Internet of things (IoT) devices dramatically increase the amount of data that needs to be protected. In addition to this, since most of the data is encrypted, this places high demands on the performance of the system. In this case, considering the higher throughput and overall capacity, enterprises will choose to prioritize business assurance, that is, not inspect or protect a certain percentage of data, which will bring greater security risks.

7.3 Inability to adapt security policies in heterogeneous cloud environments

The evolving nature of security threats and the rapid advancement of cloud computing technology present a challenge in meeting the ever-changing security demands. Cloud architectures with multiple independent CSPs encompass various components, each with distinct security requirements. Additionally, the landscape of security threats is dynamic, necessitating continuous evolution of security solutions to keep pace with emerging risks. Traditionally, relying solely on physical security products with stable security functionalities has been insufficient to adapt to the evolving security landscape.

When adopting cloud services, enterprises must fully understand and adapt to the shared responsibility model of cloud service providers. However, this model often leads to an unclear delineation of security responsibilities, posing challenges for the formulation and implementation of security policies. At the same time, the differences in security configuration requirements and best practices across different cloud platforms complicate security configuration tasks, making it easy to trigger security risks due to improper configuration. The scalability of a multi-cloud environment can help CSC meet workload processing needs by adding resources, and data can be rerouted to meet user demand. The downside of this change is that data will be transferred in unpredictable ways. Especially in today's complex and asynchronous environment, enforcing policies and protocols can quickly become a difficult task. For security management teams, a complex multi-cloud environment puts forward high requirements for managers, and a cross-cloud platform environment requires security managers to have a deep understanding of the technologies and services of different CSPs and be able to formulate a unified security strategy based on the multi-cloud architecture to deal with the security features and risks of different cloud platforms.

7.4 Security information and event management complexity

Aggregating and correlating security events and logs from multiple CSPs to generate meaningful insights is a major challenge. Different CSPs may use disparate log formats and event structures, requiring additional effort to normalize and analyse the data effectively.

In multi-cloud and hybrid cloud environments, each CSP typically collects and generates a large amount of security information, including user login activities, access requests, abnormal activities and potential security attacks. This information is usually transmitted to a centralized log management platform or a SIEM system for further analysis and response. The security information flowing between multiple CSPs and CSCs includes authentication information, access control information, security event logs, encryption and key management information, network security information, compliance and audit information, and vulnerability management information. Each type of information faces the risk of data leakage during transmission. For example, authentication information may be subject to identity theft, credential reuse and man-in-the-middle attacks.

The differences in the structure and format of security information from different CSPs can also pose security risks. In multi-cloud and hybrid cloud environments, the security information from each CSP exhibits significant heterogeneity, which is reflected in inconsistent data formats, varying data granularity and content, and non-uniform event definitions. Each CSP typically provides different log and security information formats based on its own architecture and design. These differences in format make it difficult to integrate and analyse data across CSPs. Moreover, the inconsistencies in security event definitions, severity levels and response strategies among different CSPs further complicate cross-CSP event response and analysis.

7.5 Fragmented identity and access management

Identity and access management (IAM) across multiple CSPs introduces a set of complex security challenges. Each CSP may provide its own IAM mechanisms, making it difficult to manage user provisioning, deprovisioning, authorization changes and access termination consistently across cloud platforms.

The differences in identity verification, authorization methods and access control models across various CSPs significantly complicate the management of a unified identity lifecycle across multiple platforms. Creating user identities, configuring permissions and revoking access across multiple CSPs often require these operations to be performed individually within each CSP, thereby increasing the risk of errors. If identity management operations within a given CSP experience delays or fail to sync promptly, it can lead to inconsistencies in cross-platform identity management, thus posing security risks.

Also, different CSPs may have unique access control models and policy configurations. This complicates the standardization of access policies, thereby posing challenges in creating and implementing unified access control policies across all cloud platforms. The access control models of different cloud platforms have varying definitions and management methods for permissions. For example, some cloud platforms use role-based access control (RBAC), while others use attribute-based access control (ABAC). These differentiated access control models make it more difficult to implement consistent access control policies across all cloud platforms.

Managing IAM across multiple CSPs also introduces significant challenges in security auditing and compliance. Each CSP utilizes different log formats and audit trail mechanisms, making it difficult for organizations to maintain consistent audit standards and operations across all cloud platforms. Furthermore, the compliance requirements vary between platforms, requiring organizations to ensure that all platforms adhere to relevant regulations and standards in a multi-cloud environment. This adds another layer of complexity to IAM management, as businesses must navigate the differences in audit practices and compliance needs across CSPs.

7.6 Challenges in ensuring data security and privacy compliance

The challenge in data security and privacy within a multi-cloud environment involves ensuring data confidentiality, integrity and availability across diverse CSPs. To address confidentiality concerns, organizations must implement robust encryption measures for data at rest and in transit, coupled with stringent access controls, audit and logging mechanisms to thwart unauthorized access. Maintaining data integrity requires the capability to detect and rectify corrupted data across multiple cloud providers. Ensuring data availability mandates the ability to access data seamlessly even during outages of one cloud provider, demanding the establishment of comprehensive disaster recovery plans.

Ensuring data confidentiality is complex in a multi-cloud environment. The fact that multiple CSPs adopt different encryption standards, authentication mechanisms and access control policies makes it difficult to uniformly implement data encryption and access control. The integrity and availability of data are also affected by the multi-cloud environment. Differences in data storage and processing mechanisms among multiple CSPs make it challenging to ensure data consistency and accuracy. This

is because any risk of damage or tampering during data transmission or replication between platforms can impact business operations.

In summary, data confidentiality, integrity and availability are core requirements in a multi-cloud environment. Enterprises must address these challenges through encryption, access control, disaster recovery planning and compliance management. Additionally, particular attention must be given to data sovereignty and cross-border data flow to ensure that data meets technical requirements.

7.7 Lack of secure and seamless interoperability

Ensuring secure integration and interoperability between different cloud services in multiple cloud environments can be complex, as cloud providers may use different operating systems, programming languages and database systems. This can make it difficult to develop applications that can be deployed across multiple cloud providers.

First, there are significant differences in the security models of various cloud platforms, which pose challenges when operating across platforms. In terms of identity verification and authorization mechanisms, different CSPs may employ distinct identity management systems, access control policies and authentication protocols. Data exchange and communication between cloud services also present security concerns. When transmitting data across multiple CSPs, incompatibilities in network architectures, encryption protocols and data protection measures between platforms can increase the risk of data breaches, tampering or loss.

Next, the integration of resources and services across platforms may introduce operational security vulnerabilities. Service interfaces, APIs and integration points are often targets for attacks. If services and applications across different cloud platforms are not adequately security-tested, cross-platform calls and data exchanges may become sources of vulnerabilities. In traditional single-cloud environments, enterprises can rely on the built-in security monitoring tools of CSPs. However, in multi-cloud environments, organizations need to integrate security monitoring systems from different platforms. Since each CSP has different security tools and alert mechanisms, it is more challenging to unify and coordinate the handling of cross-platform security incidents.

In conclusion, achieving security interoperability in a multi-cloud environment is highly complex. Enterprises need to address multifaceted challenges, including authentication, data exchange, API integration, cross-platform security monitoring and compliance. Only through refined security policies, technical measures, automation tools and cross-platform collaboration mechanisms can security and efficient interoperability be realized in a multi-cloud environment.

8 Framework for a cloud-native-based security collaboration mechanism

The cloud-native-based security collaboration framework addresses the challenges identified in clause 7 through three complementary capability areas: unified security management, collaboration on security solutions and flexible security features.

In the cloud-native-security collaboration framework, the parties involved in the collaboration are not limited to CSPs and CSCs. It also includes third-party security tools and service providers, who can offer specialized services such as security detection, vulnerability scanning and threat intelligence, further enhancing overall security defence. At the same time, the development and operations teams need to ensure the security of code, applications and infrastructure during deployment and management, working with the security teams to take preventive measures and conduct risk assessments. Compliance teams are responsible for coordinating compliance checks across different cloud platforms, ensuring adherence to local laws and industry standards, and responding to and adjusting to regional data protection regulations.

Only when all parties involved in this security collaboration mechanism work closely together and coordinate consistently, as shown in Figure 1, can they ensure the consistency and interoperability of

security functions across cloud environments and achieve strong security protection in complex and ever-changing cloud environments.

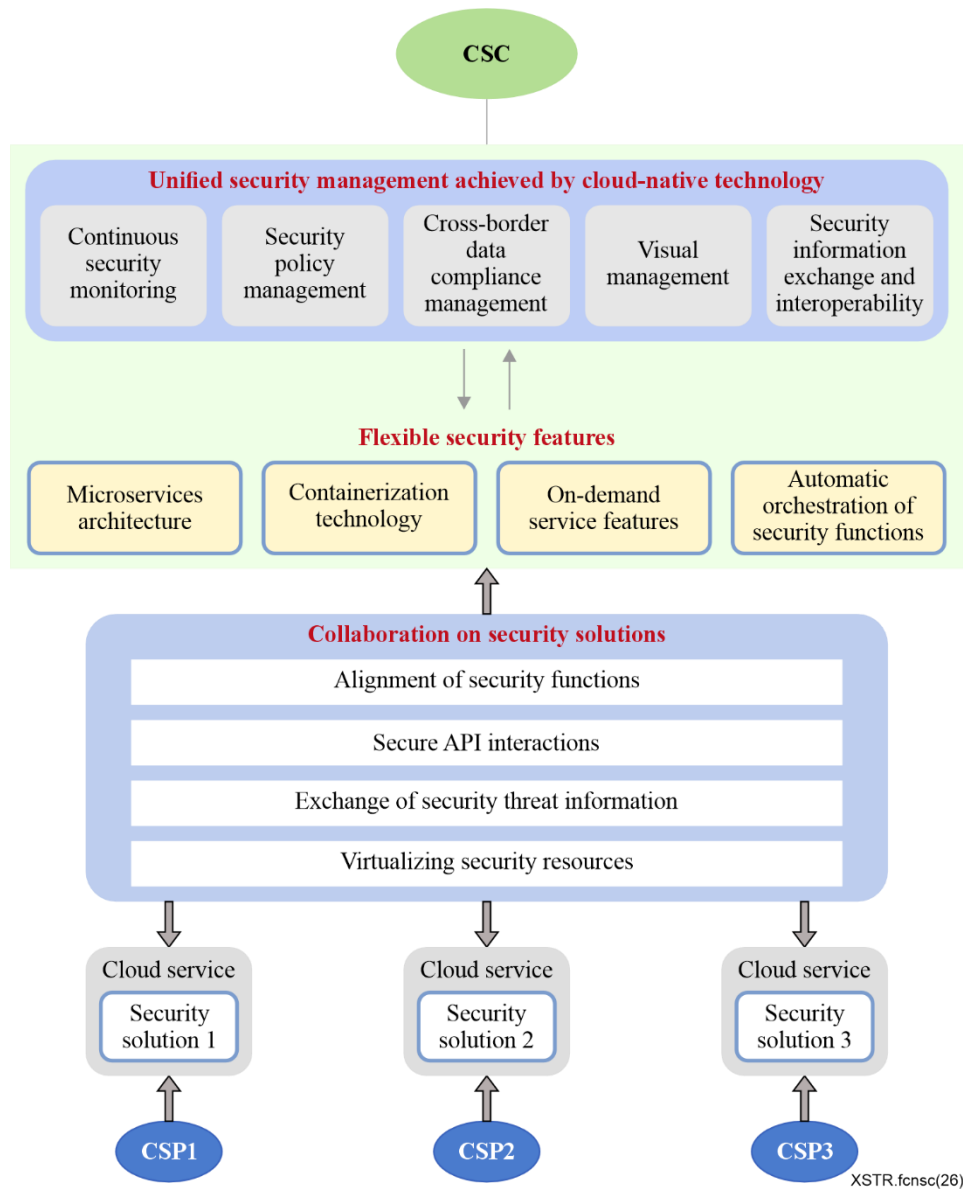


Figure 1 – Security solutions in the cloud with multiple CSPs

8.1 Unified security management

The framework provides a comprehensive view of cloud security across multiple CSPs by supporting unified management and monitoring. Within the cloud-native-based security collaboration mechanism, common rules are established for recording, exchanging and processing security threat information so that security functions and related information can be collected, correlated and managed in a coordinated manner.

In a multi-cloud environment, unified security management faces many challenges. Different CSPs typically have independent security tools and management platforms, making it difficult to implement cross-platform security strategies and policies consistently. Therefore, to achieve unified security management, cross-platform collaboration, policy standardization and deep integration of security features from various CSPs are required.

8.1.1 Continuous security monitoring

By employing log auditing and behavioural monitoring methods, security awareness can be enhanced. Utilizing log auditing and behavioural monitoring systems, long-term and continuous monitoring and oversight of multiple cloud services can be achieved. The appropriate automation tools should be used to maintain persistent surveillance over multi-cloud systems, ensuring that any security threats are promptly detected, reported and addressed.

To implement effective log auditing and behavioural monitoring in a multi-cloud environment, it is essential to first establish a cross-platform log governance framework. By standardizing the collection of logs from various CSPs and unifying heterogeneous data into a common format, semantic differences between various logs can be addressed. Additionally, to enhance monitoring and protection of critical points within cloud platforms, lightweight probes should be embedded at key control points to enable the end-to-end tracking of network traffic and application behaviours, ensuring that no monitoring blind spots exist. This approach ensures the operational quality of the cloud platforms.

Security information and event management (SIEM) is a comprehensive security management solution designed for real-time monitoring, analysis and response to security events and threats within a network. To enable continuous security monitoring, SIEM solutions can be deployed in multi-cloud environments to centrally process security alerts and log data from various cloud platforms, thereby enhancing the efficiency of security operations. SIEM tools heavily rely on log data and require the standardization of the granularity of services provided by different CSPs in order to ensure security visibility.

8.1.2 Security policy management

Security policy management in a multi-cloud environment requires the unification of cross-platform mechanisms such as access control, identity authentication and data protection, ensuring the consistent implementation of security standards and response strategies across different cloud platforms.

- 1) Access management should provide unified identity authentication for the CSC, although the cloud services used by a CSC may come from multiple CSPs, authentication data should be passed from access management to multiple related CSPs; in addition, multi-factor authentication is required to enhance security.
- 2) Users should adopt a zero-trust approach to access control, users should provide access rights according to their needs, and no more permissions should be assigned in addition. The zero-trust approach can not only protect some important data with high confidentiality but also clearly understand which user accessed the data and when the user accessed the information, which also greatly reduces the difficulty of management by operations and maintenance personnel. Enable IAM integration across cloud platforms to centrally manage user identities and access.
- 3) Adopt fine-grained access control. To reduce the burden of security management and provide a simpler workflow for developers, each microservice should only have the minimum set of permissions required to complete its functionality. In addition, the service mesh technology can also be used to further constrain each microservice and standardize its behaviour pattern.
- 4) By establishing a scientific data classification standard and mapping it to the access control models of each CSP, the complexity of policy configuration can be significantly reduced, mitigating security risks caused by cognitive biases related to data sensitivity. Categorizing data into different levels of sensitivity helps determine the importance and confidentiality of the data, thus simplifying access decisions across different CSPs.
- 5) A multi-cloud API strategy should be developed to manage microservices distributed across the multi-cloud environment in a logically unified manner. Instead of requiring CSPs to modify their native APIs, the strategy can introduce an API gateway or mediation layer that

maps heterogeneous provider-specific APIs to a consistent set of security capabilities for collaboration. The API management policy may include the use of common interface descriptions and harmonized identity authentication and authorization mechanisms for the exposed multi-cloud security collaboration APIs, while also considering API performance management and lifecycle management.

8.1.3 Cross-border data compliance management

A unified data management capability should support data migration, synchronization, backup and recovery while maintaining data integrity, consistency and traceability. In multi-cloud and hybrid cloud environments, this capability should also support compliance-management controls for cross-border data transfer, including policy enforcement, auditability and location-aware handling of security-relevant data.

- 1) Use cloud-native network policies and tools to manage network traffic and security in a multi-cloud environment. Adopt microservice architecture and containerization technology to achieve secure communication between microservices and fine-grained traffic management. Leverage cloud-native network policy controllers to create an isolated network environment that ensures that only legitimate traffic can flow between services.
- 2) CSC needs to build a strong partnership with CSP and work together to develop and implement security protocols. Threat intelligence information should be shared among CSPs on a unified data management platform. In addition, enterprises should proactively implement continuous monitoring and evaluation of the security performance of CSPs to ensure that they continue to meet industry security standards. In this way, security risks can be more effectively prevented and the overall security management level can be improved.
- 3) Through a unified data management platform, it can fully integrate infrastructure as a service (IaaS), platform as a service (PaaS) and traditional devices to achieve unified operation and maintenance and business operation services. By integrating existing database and network resources, the framework creates a centralized virtual pool of information resources, so as to realize the centralized management, operation, maintenance and business operation of resources, which not only improves the efficiency of resource utilization but also promotes the sustainable development of the organization. By consolidating pools of virtual, storage and network resources, a wide range of virtualization use cases can be supported, from public to private to hybrid clouds.

8.1.4 Visual management

Through aggregating various security data in a multi-cloud environment, the visualization system forms a unified situational awareness capability, transforming fragmented security information into intuitive visual presentations. For visual management in multi-cloud environments, a visualization-level data format or schema can be defined to describe security data such as logs, alerts, metrics and asset status in a consistent manner. Heterogeneous data from different CSPs can be transformed into this format through normalization and mapping mechanisms for unified visualization.

- 1) Enterprises should select cloud service platforms that can provide the required computing power, storage options, network functions and integration with other services or APIs. By deploying a unified management interface, enterprises can visualize data across multiple cloud environments and monitor resource usage, performance metrics and security alerts, thereby helping enterprises quickly locate security issues.
- 2) In multi-cloud and hybrid cloud environments, enterprises should ensure that all data stored and processed on the cloud platform meets industry standards. Deploy a variety of security measures, including data encryption, access control, security event monitoring and regular security audits.
- 3) Monitor and optimize cloud spending with cost management tools such as cloud cost analysis and budget monitoring. Implement automatic resource optimization, automatically monitor

some low-frequency cloud resources and allocate cloud resources on demand through appropriate scheduling to further reduce costs and maximize benefits.

- 4) Record the historical data of the system, with the help of machine learning algorithms and trend analysis to identify potential security threats. Collect feedback from users on a regular basis to improve the visualization tool based on the feedback.
- 5) Set up disaster recovery plans and backup mechanisms for key business processes to reduce the risk of single points of failure. Through redundancy design and load balancing, requests are distributed across ECSs, which not only improves performance but also prevents problems caused by single node failures.

8.1.5 Security information exchange and interoperability

A unified security information exchange format can effectively facilitate the flow of security information between different CSPs, laying the foundation for unified security management.

When standardizing the security information exchange format, the types of security information should cover the following major categories: log and event data (such as user operation records, network traffic logs), security event alerts (including intrusion detection results and compliance violations), asset and configuration data (such as cloud resource inventory and security policy status), threat intelligence (such as malicious IPs and attack patterns), identity and access data (such as cross-cloud user permission change records), and vulnerability and patch information (such as Common vulnerabilities and exposures (CVE) details and patch progress). These pieces of information should be described using standardized fields to ensure consistency across platforms.

In the process of developing a unified security information exchange format, it is crucial to conduct in-depth research on data protection requirements across different jurisdictions. The flow of security information must support bidirectional interaction and cross-platform collaboration. From CSP to CSC, the information flow is reflected in the real-time push of security alerts or compliance reports. The reverse flow involves customers submitting custom security policies or sharing threat intelligence with the CSP, such as generating detection rules via policy definitions and synchronizing them across multiple cloud platforms. Furthermore, information sharing across CSPs must overcome platform heterogeneity, potentially using open and standardized data models to achieve log format compatibility, thus supporting attack chain tracking across different cloud platforms.

In practice, enterprises can achieve end-to-end management through toolchain integration. This process not only enhances threat detection efficiency but also reduces the risk of configuration errors through unified policies. In conclusion, the core of a unified exchange format lies in compatibility, scalability and security, ultimately breaking down data silos and enabling multi-cloud collaborative defence.

8.2 Collaboration on security solutions

The framework enhances collaboration among security solutions across multiple CSPs in order to improve security response efficiency. Based on common rules for security threat information exchange and security-function interaction, the cloud-native-based security collaboration mechanism supports automated exchange of security threat information and coordinated interaction through API mediation and orchestration capabilities.

To ensure secure interoperability between multiple cloud platforms, organizations must carefully integrate and coordinate the mechanisms of each cloud platform, ensuring consistency in IAM across clouds. In addition, to ensure the secure transmission of data between different cloud platforms, companies need to protect the confidentiality and integrity of data during transmission, while complying with the relevant laws and regulations of different countries and regions, especially those concerning cross-border data transfers. Companies must also ensure that each cloud platform is capable of proper auditing and logging to trace cross-platform data exchange activities and detect

potential security threats in a timely manner, while adhering to data privacy protections and regulations on cross-border data transfers.

To ensure the security of services across platforms, organizations must strengthen auditing of all service interfaces, ensure the security of APIs, and implement stringent authentication and authorization mechanisms. Additionally, measures should be taken to encrypt communications and monitor traffic across cloud services to prevent API abuse or malicious attacks. Enterprises need to ensure that data flowing across platforms complies with all relevant requirements, including regulations on data encryption, data access control and data storage location.

8.2.1 Alignment of security functions

- 1) Industry security standards and best practices should be developed and adhered to ensure that the security measures provided by different CSPs are compatible with each other, so that better collaboration can be achieved.
- 2) CSPs should also establish appropriate access control when aligning security functions. The access control strategy should take a zero-trust approach and follow the principle of least privilege, providing access to the user's needs without assigning more permissions. Access control can well protect some important data with high confidentiality, and the least privilege assignment can prevent more security problems.
- 3) Multiple CSPs should collaborate and fully consider compatibility during the design phase, while also developing a cross-cloud security incident response plan to ensure a fast and effective response when security incidents occur. Given the differences between CSPs, it is crucial that their security functions and policies are designed to work together to avoid vulnerabilities or delays in security management caused by platform disparities. Additionally, communication protocols between CSPs should be clearly defined so that critical information can be shared promptly in the event of an incident, ensuring smooth communication and avoiding delays due to miscommunication or information lag. When allocating security functions, each CSP should establish detailed security incident response strategies and procedures, including roles and responsibilities, response workflows and communication protocols.
- 4) After a security incident occurs, each CSP should promptly share security threat intelligence while ensuring compliance and data privacy, collaborating to identify gaps in the response process in order to better address and analyse threats in a multi-cloud environment. During the security incident response, CSPs should collaboratively identify and assess shortcomings in the existing response procedures, make timely adjustments and optimizations to the response measures and jointly prepare security reports to provide valuable insights for the development of future security strategies.

8.2.2 Secure API interactions

- 1) The multi-cloud platform needs to provide APIs to the outside world to provide extended functions, provide support and be compatible with other cloud platforms. The multi-cloud management platform provides APIs to develop and deploy your own management policies, so as to quickly complete the expansion of business functions.
- 2) Cloud-native technologies can facilitate collaboration between different security solutions through standardized APIs and service discovery mechanisms. In multi-cloud environments, cloud-native service meshes can provide a unified framework for secure communication between different cloud platforms. Service mesh technologies can support encrypted transmission, centralized management of cross-platform authentication and authorization policies and coordinated interaction among security functions.
- 3) Use API management tools to provide unified API management across cloud and on-premises, optimize API communication flows and meet security and compliance requirements. API management tools should provide real-time monitoring and logging

capabilities to identify and resolve performance issues or security vulnerabilities in a timely manner. These capabilities should be able to work across multiple cloud environments.

- 4) Adopt a strong security authentication mechanism. When interacting with the APIs of other CSPs, in addition to ensuring the security of data transmission through the HTTPS protocol, additional measures need to be taken to verify the authenticity of the client's identity to prevent data tampering. To do this, each API request should be accompanied by the signature of the user account. This signature can be generated by the hash-based message authentication code (HMAC) algorithm and should be sent as part of the HTTP request header. This method not only ensures the encryption of the communication but also verifies the integrity of the request and the authenticity of the source through the signature mechanism.

8.2.3 Exchange of security threat information

- 1) Establish a security threat information-sharing platform. Each CSP should summarize the network security threat information data provided by various channels on the security threat information-sharing platform, establish a fair information evaluation system, promote the development of information sharing and curb the flood of threat information in the network.
- 2) In a multi-cloud environment, there needs to be a unified strategy to manage the security measures of different CSPs. This includes having a business continuity and disaster recovery plan in place, using data loss prevention tools and ensuring you have a comprehensive understanding of what is happening in your cloud environment.
- 3) Generally, CSPs are responsible for the security of cloud infrastructure, while CSCs are responsible for the security of data and applications in the cloud. In multi-cloud and hybrid cloud environments, the security responsibilities of each CSP need to be clearly defined.

8.2.4 Virtualizing security resources

Virtualization is one of the key technologies for enabling hybrid cloud, allowing users to create multiple virtual machines on a single physical server, each of which can run different operating systems and applications.

Virtualizing security resources can guarantee the application of microsegmentation. Microsegmentation is a network security management approach that manages network access across workloads by dividing the network into subsegments and applying security controls based on the security needs of each segment. This approach leverages a zero-trust architecture and adheres to the principle of least privilege, allowing administrators to precisely manage security policies, limit traffic, effectively reduce the attack surface, and strengthen protection against data breaches.

Microsegmentation uses network virtualization technology to create security zones in cloud deployments that are small security zones that isolate workloads and tailor security policies to each workload. This granular level of security control is critical for modern cloud environments running multiple applications. Instead of adopting a unified security policy for servers, organizations can apply security controls individually for each workload and application.

Service mesh technology can be used for secure communication between microservices across multiple CSPs. It achieves a secure interconnection of cloud services by automatically providing identity authentication, access control and encryption for each microservice. Service mesh is particularly crucial in cloud-native architectures as it helps manage the communication security between large-scale distributed services.

The need for cloud-native security is reflected in new components facing new risks, such as containers that are not as isolated as virtual machines, making them more susceptible to escape attacks. By leveraging virtualization technology, collaboration between multiple CSPs can be enhanced.

8.3 Flexible security features

The framework provides flexible security features on demand. Cloud-native-based security collaboration mechanisms provide security functions as smaller and independent microservices, follow common rules for security threat information exchange and function interaction, and support the orchestration of security functions according to the security characteristics of multi-cloud and hybrid cloud environments. Flexibility should be implemented within applicable compliance requirements so that dynamic security capabilities remain auditable and policy controlled.

8.3.1 Microservices architecture

Cloud-native security collaboration mechanisms provide security capabilities by providing smaller, independent microservices. A microservices architecture needs to be easy to deploy across different CSPs, with each service being a small, independent functional module that can be developed, deployed and scaled independently, while enabling modularity of security functions. Microservices architecture allows new functionality to be added to legacy systems without having to change the entire system. The basic features of a complete microservices system base should include the following:

- API gateway: serves as the entry point to the microservice system and handles request routing, load balancing, authentication and authorization.
- Configuration management: Centrally manages the configuration information of microservices and supports dynamic update of configurations.
- Service communication: Services interact with each other through lightweight communication protocols.
- Containerization: Use container technologies such as Docker to encapsulate services to ensure environmental consistency and easy deployment.
- Container orchestration: Use Kubernetes or other container orchestration tools to manage the lifecycle, scaling and automatic recovery of containers.
- Continuous integration/continuous deployment (CI/CD): Automate code build, test and deployment processes to iterate and release services quickly.
- Monitoring and logging: Integrate the monitoring system and log system to monitor service status and collect logs in real-time.
- Distributed tracing: Use a distributed tracing system (such as Zipkin) to monitor and diagnose the call chain between microservices.
- Service mesh: Provides intelligent routing, fault recovery and secure communication between microservices.
- Security policy: Implement unified security policies, including inter-service authentication, authorization, data encryption and security hardening.
- Fault tolerance: Implement circuit breaker mode, retry mechanism and circuit breaker mechanism to improve system availability and fault tolerance.
- Multi-cloud and hybrid cloud support: Ensure that microservice systems can be flexibly deployed and run in multi-cloud and hybrid cloud environments.
- Automated testing: Implement automated testing, including unit testing, integration testing and performance testing.
- Business requirements analysis: Ensure that microservices are designed to meet current and future business needs.
- Technology stack selection: Choose the right technology stack based on service needs and team skills.

8.3.2 Containerization technology

Cloud-native technologies can further enhance security by integrating runtime protection measures for containers. These technologies can detect abnormal behaviour, unauthorized access to resources and other security risks during container runtime, helping enterprises identify potential security threats in real-time. By leveraging containerization technologies such as Docker and container orchestration tools, organizations can deploy and manage microservices, ensuring the consistency and portability of applications across different environments.

- 1) The benefits of using containerization technology include its cross-cloud platform support. One of the biggest benefits of containers is their adaptability; more and more cloud platforms support containers, users no longer need to worry about being tied to cloud platforms, and it is possible to deploy applications across multiple platforms. At present, many mainstream IaaS cloud platforms support containers.
- 2) The design of container images should be platform-independent, allowing them to run on multiple operating systems such as Windows, Linux and macOS, thus enhancing the portability of applications. Once the image is built, it needs to be stored in a container registry for easy management and distribution. At the same time, container images stored in the registry should be uniformly managed to prevent high-risk vulnerabilities from emerging in these images.
- 3) Containers must have strong isolation to ensure that they do not interfere with or affect each other. In a multi-cloud environment, the application isolation provided by containers forms the foundation of security, preventing potential security vulnerabilities from spreading between different services. If there is insufficient isolation between containers, attackers could compromise the entire application system through one container. Therefore, containers should support resource isolation and runtime permission restrictions to ensure the security of each container.
- 4) Ensure the isolation of containers, image security and runtime security. Use container isolation technology and perform security scanning and real-time monitoring of container images to prevent malicious code or vulnerabilities. In addition, it is best to use a trusted mirror source for security.
- 5) Containers face various security threats during runtime, including malicious processes, unauthorized access and malicious network communication. Therefore, containerization technology must have runtime security monitoring capabilities to detect abnormal behaviours and potential attack activities in real-time. The security of container runtimes can be enhanced by using minimal base images, resource limitations and security context isolation. Additionally, enterprises should use container security tools to monitor processes, file systems and network traffic within containers, enabling the timely detection of anomalies and the implementation of necessary protective measures. Moreover, access control for container runtimes must be strengthened to ensure that only authorized users and services can access sensitive data and resources.

8.3.3 On-demand service features

With the on-demand service characteristics of cloud-native architecture, service providers can dynamically support resource scheduling, container orchestration and auto-scaling services, enabling businesses to respond more flexibly and efficiently to ever-changing business needs.

- 1) Real-time monitoring of the security performance and resource utilization of microservices: Leveraging the elastic scaling capabilities of cloud-native platforms to monitor the load conditions of various cloud platforms in real-time. By using load balancing strategies, dynamically adjust resource allocation based on real-time load and performance metrics, directing requests to the cloud platform with lower load, ensuring efficient service operation and optimizing application performance and cost-efficiency.

- 2) By centrally monitoring and analysing network logs and activity data, security orchestration, automation and response (SOAR) platforms can help organizations effectively identify and respond to potential malicious activities, while updating protection measures to maintain network security. At the same time, automated systems enable organizations to stay ahead and take necessary preventive measures by predicting emerging risks and threats, ensuring information security.
- 3) Backup and disaster recovery are key functions to ensure data security and availability. The on-demand service functionality can automatically perform data backup or recovery operations based on actual needs, ensuring that in the event of failure or disaster, business operations can quickly resume and prevent data loss. In a multi-cloud environment, enterprises can configure automatic backup policies to automatically back up data to multiple cloud platforms based on real-time service load or data changes. When a failure occurs in one cloud platform, the system can automatically restore from backups on other cloud platforms, ensuring business continuity.

8.3.4 Automatic orchestration of security functions

Cloud-native technologies enable adaptive security policies that dynamically adjust security defences based on changes in the environment and traffic patterns. By using automation tools and cloud-native technologies, security responses can be automatically triggered and executed based on detected security threats. Automated security functions help security teams monitor network security events and respond to them, accordingly, enhancing the overall responsiveness and efficiency of security management.

- 1) Automation should follow continuous integration and continuous delivery (CI/CD) pipelines. It can automatically build, test, deploy and release applications, speeding up delivery and reducing manual tasks. CI/CD, which includes continuous integration and continuous delivery, requires automation, such as build, test and static code analysis, to frequently integrate developers' code changes into a shared code repository. After that, automated processes deploy the tested code into the production environment.
- 2) A standardized approach to security information exchange enhances the flexibility of security-function orchestration. By defining common descriptions for logs, alerts, threat intelligence and asset data across different CSPs, organizations can enable seamless information flow between platforms. This allows security functions — such as policy enforcement, threat detection and incident response — to be orchestrated across cloud environments without being locked into proprietary formats. For example, detection rules generated through policy-as-code tools can be synchronized across multiple cloud platforms, supporting flexible and coordinated security operations.
- 3) Allow CSC to customize security features to meet its specific requirements. To address emerging threats, provide CSC with an interface or API that allows real-time adjustments to security policies and rules. Use configuration management tools to achieve centralized management and dynamic updating of application configurations, and automatically apply security hardening measures. Provide interfaces and tools to extend existing security features or add new capabilities, ensuring that the security collaboration framework can adapt to new security challenges and technologies.

Bibliography

- [[b-ITU-T Y.3500](#)] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.
- [[b-ITU-T Y.3527](#)] Recommendation ITU-T Y.3527 (2021), *Cloud computing - End-to-end fault and performance management framework of network services in inter-cloud*.
- [[b-ITU-T Y.3532](#)] Recommendation ITU-T Y.3532 (2023), *Cloud computing - Functional requirements of Platform as a Service for cloud native applications*.
- [[b-ITU-T Y.3537](#)] Recommendation ITU-T Y.3537 (2022), *Cloud computing – Functional requirements of a cloud service partner for multi-cloud*.
-