# Huawei Cloud Data Security White Paper

**Issue** 3.0

**Date** 2025-03-03

**HUAWEI TECHNOLOGIES CO., LTD.**

### Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Email: support@huawei.com

# Contents



# 1 Overview

Data is as a new production factor and the foundation for enterprises' digital and intelligent transformation. As businesses accelerate their digital and intelligent transformation, the demand for cloud computing services continues to grow. This brings both significant development opportunities and numerous challenges, especially in data security. Risks like sensitive data breaches, ransomware attacks, and data use violations have become major concerns for companies migrating to the cloud.

Huawei Cloud, as a responsible cloud service provider, understands the significance of data security and views it a crucial element to business growth. Huawei Cloud has established a comprehensive data security governance system, encompassing organizational structure, policies & systems, process specifications, technical tools, and measurement & supervision, to provide systematic security assurance for customer data. Internally, Huawei Cloud continuously enhances security technologies and management measures, implementing a multi-layer protection system to ensure end-to-end data security compliance. Externally, Huawei Cloud offers comprehensive security services and features throughout the lifecycle, and obtains data protection certifications from independent third-party organizations to demonstrate its high standards and ongoing effectiveness in data security practices to the industry.

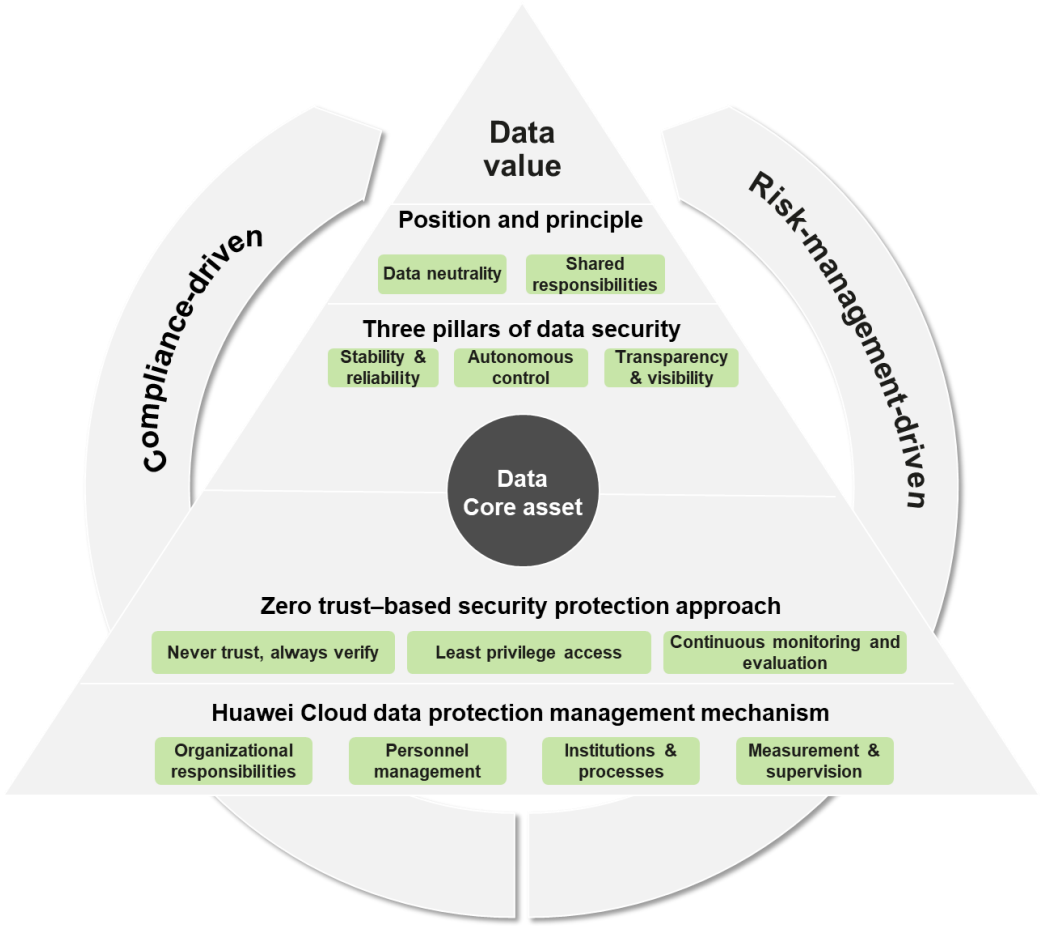
To further address customers' security concerns about migrating data to the cloud, Huawei Cloud continues to adhere to the principle of "data neutrality" and maintains that "customers own and use their data." It never uses technical means to access customers' business data and never forces customers to exchange data with Huawei Cloud, and ensures that all data processing strictly complies with laws and regulations. Huawei Cloud helps customers leverage data for value creation and build secure, controllable cloud data security protection capabilities.

Additionally, to better safeguard customers' personal information and assist them in establishing privacy protection for their cloud services, Huawei Cloud has developed a comprehensive privacy protection management system to ensure consistent and effective privacy protection. For more information, refer to the *Huawei Cloud Privacy Protection White Paper* in the **Privacy** module in **Trust Center**.

# 2 Huawei Cloud Data Security Architecture

**Figure 2-1** Huawei Cloud data security architecture




Huawei Cloud adheres to the principle of "data neutrality" and firmly believes that "customers own and use their data, and Huawei creates value for them." Focusing on data assets and driven by compliance and risk management, Huawei Cloud has established a data security system based on the principles of "never trust, always verify," "least privilege access," and "continuous monitoring and evaluation." This

system is supported by three pillars: stability & reliability, autonomous control, and transparency & visibility.

Huawei Cloud's data protection management mechanism encompasses four aspects: organizational responsibilities, personnel management, institutions & processes, and measurement & supervision, thereby providing fundamental guarantee to systematically and effectively protect customer data and help achieve data security objectives.

Huawei Cloud protects customers' cloud data assets through three pillars: stability & reliability, autonomous control, and transparency & visibility. Specifically,

- Stability & reliability: Huawei Cloud provides a stable and reliable cloud platform infrastructure that ensures the security of content data on the cloud in three states — data at rest, data in use, and data in transit.
- Autonomous control: Huawei Cloud offers full-stack data security services and features, enabling customers to independently decide data residency locations and data migration to/from the cloud, and implement security management throughout the data lifecycle based on their specific security needs.
- Transparency & visibility: Huawei Cloud offers transparent and visualized data processing capabilities, enabling customers to gain a deeper understanding of the processing of content data on the cloud, including management of authorization for remote customer service support and operations involving content data.

In the complex cloud service business model, data security is a shared responsibility between customers and Huawei Cloud. To ensure data security, Huawei Cloud follows common industry practices and combines them with specific use cases to define the responsibilities and obligations of both parties. This helps customers understand the boundaries of data protection responsibilities and avoids data protection gaps.

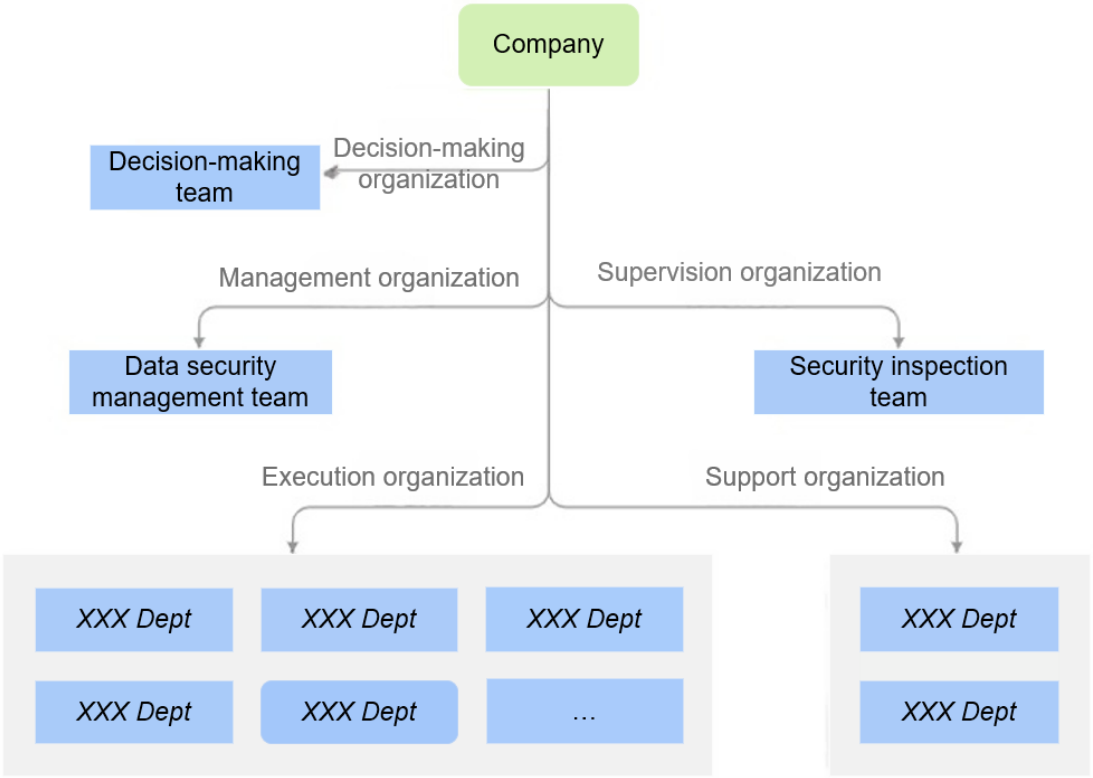
# 3 Huawei Cloud Data Protection Governance System

## 3.1 Organizational Responsibilities

Huawei Cloud has established a comprehensive data security management responsibility system that encompasses decision-making, management, execution, supervision, and support levels. This system serves as a crucial framework to ensure that cloud content adheres to data security standards. By clearly defining responsibilities and collaboration mechanisms at each level, Huawei Cloud not only strengthens its internal security management process but also enhances trust with users, ensuring transparency and compliance of data processing activities. At each level, security policies and operation guidelines must be strictly followed to prevent data breaches, safeguard user privacy, and preserve system integrity, thereby offering robust data security protection for both businesses and individual users. The data security management responsibility system is indispensable to the company. It specifies responsibilities at each level, the security incident response process, and how to continuously improve security measures.

**Figure 3-1** Huawei Cloud data security management responsibility system



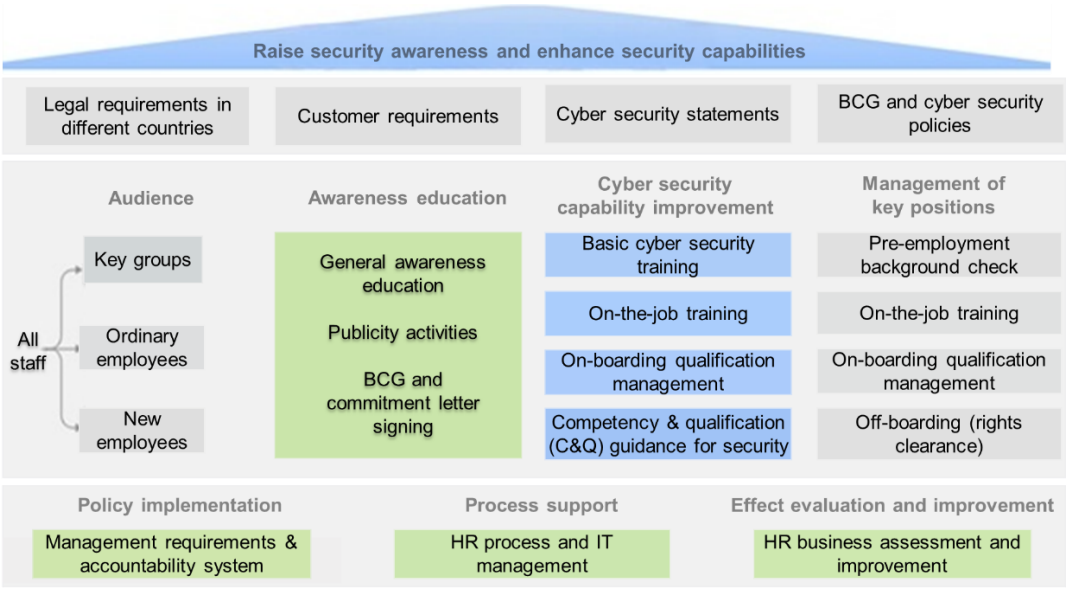

- Decision-making: The decision-making team is responsible for making decisions on Huawei Cloud data security strategies and major issues.
- Management: The data security management owner and organization are responsible for routine data security management, communication with external regulators, and trust & capability building.
- Execution: The data security owner is responsible for implementing data security requirements and conducting routine data security management within their domain and is accountable for the results of data security in that domain.
- Supervision: An independent inspection team is appointed to promote data security. The team verifies the data security work of each business domain, and urges data security owners in each business domain to track and manage identified issues in a closed-loop manner.
- Support: There are organizations established to support data security operations, including tool development, personnel capability development, and external communication.

## 3.2 Personnel Management

Huawei Cloud implements a comprehensive personnel security management mechanism, including regular security training, strict access control, and clear security responsibility assignment. These measures not only enhance the security literacy of both internal personnel and contractors but also ensure that all operations adhere to high standards of security practices, thereby effectively preventing internal and external security threats and safeguarding data security.

**Figure 3-2** Huawei Cloud data security management mechanism




Huawei Cloud has established a comprehensive security management system for employees and contractors, covering the entire lifecycle from onboarding to resignation. By continuously enhancing data security awareness and capabilities of relevant personnel, Huawei Cloud effectively ensures the overall security level of the cloud platform. All staff must adhere to employee behavior management guidelines after onboarding. Anyone who breaches security requirements will face consequences in accordance with the security violation accountability mechanism. Additionally, Huawei Cloud provides regular security awareness and capability training for all staff. Employees in different positions must also undergo specific cyber security and privacy protection training to mitigate security and privacy risks caused by insufficient awareness and capabilities.

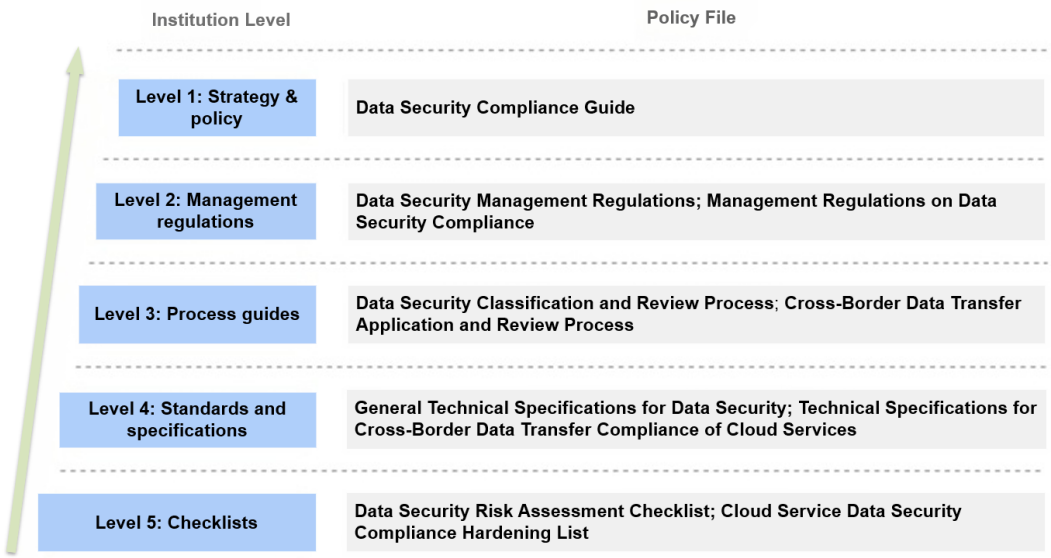
Some of Huawei Cloud services used by customers might be provided by Huawei Cloud and suppliers together. Huawei Cloud conducts security due diligence before partnering with suppliers and contractually bind them to adopt security measures to protect customer data. Huawei Cloud also formulates information security management regulations for outsourcing suppliers, includes these as additional clauses in contracts, and specifies the penalties for any violations by suppliers.

## 3.3 Institutions & Processes

To ensure effective implementation of data security management requirements, Huawei Cloud integrates these requirements into its main business processes, such as R&D, O&M, operations, supply chain, marketing and sales, engineering delivery, and technical services, enabling continuous and effective execution of these requirements. This includes developing comprehensive security policies, operation guides, and emergency response plans, which are regularly reviewed and updated to keep the security management mechanism up-to-date and adaptive to the evolving threat landscape, ensuring the security and compliance of user data.

**Figure 3-3** Huawei Cloud data security management system



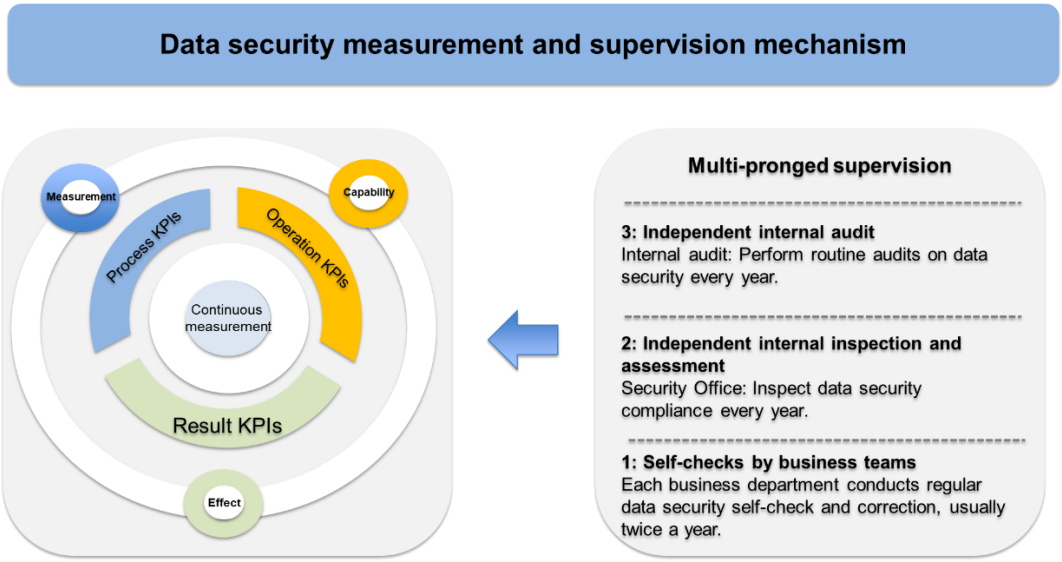

Dedicated data security processes are established, such as a data security level review process. Additionally, security requirements are integrated into existing business processes to ensure that they are not implemented separately. For instance, data security requirements are incorporated into R&D and O&M processes. Security, which is a basic requirement in the quality management system, is effectively ensured through management systems and technical specifications. Huawei monitors and improves its business processes through internal audits as well as security certifications and audits by independent third-party agencies.

## 3.4 Measurement & Supervision

Huawei Cloud has designed a comprehensive security measurement and supervision mechanism to ensure effective data security management. This mechanism encompasses all aspects from routine monitoring to advanced auditing. Through continuous tracking of key performance indicators (KPIs), potential security threats can be promptly identified and mitigated.

**Figure 3-4** Huawei Cloud data security measurement and supervision mechanism




Huawei Cloud has developed KPIs from three dimensions: measurement, capability, and effect. These KPIs are classified into process, operation, and result KPIs. Using these KPIs, Huawei Cloud can continuously evaluate and monitor the execution of data security controls and drive sustained optimization and enhancement across business domains.

Huawei Cloud has also established a three-pronged verification approach to data security supervision.

- The first verification is performed by frontline business teams. A data security specialist from each business domain regularly organizes business personnel to conduct self-check and correction based on the corresponding checklist.
- The second verification comes from an independent security inspection team of Huawei Cloud. The security inspection team conducts routine data security inspections on key business every year and is responsible for tracking and closing identified issues.
- For the third verification, an independent audit team of Huawei Group conducts spot checks on key business or domains every year as required and performs data security audits.

This multi-pronged supervision mechanism not only strengthens Huawei Cloud's security defenses but also offers customers a higher level of data security assurance, ensuring that security requirements are stringently applied in real-world operations.

# 4 Overview of Huawei Cloud Data Security Solution

Huawei Cloud builds data security services and features, focusing on data assets throughout the entire data lifecycle, to help customers achieve autonomous control over data security.

| Principle | Capability | Sub-capability | Capability or Product |
|---|---|---|---|
| Stability & reliability | Security of data at rest | Data reliability | • Assurance for storage service reliability<br>• Assurance for service reliability |
| | | Data isolation | • Virtual compute resource isolation<br>• Network isolation<br>• Service isolation |
| | | Storage encryption | • Encryption of data at rest |
| | | Secure data destruction | • Logical destruction of data<br>• Physical destruction of data |
| | | Access control | • Separation of duties (SOD) of O&M personnel<br>• Role-based access control (RBAC)<br>• Attribute-based access control (ABAC)<br>• Multi-factor authentication (MFA) and audit |
| | Security of data in transit | Transmission encryption | • Virtual private network (VPN)<br>• Application layer TLS and certificate management |

| Principle | Capability | Sub-capability | Capability or Product |
|---|---|---|---|
| | | Stable and reliable transmission | • Direct Connect |
| | Security of data in use | Confidential computing | • QingTian virtualization platform |
| | | Homomorphic encryption | • Homomorphic encryption technology |
| | | Multi-party encryption | • Multi-party computation (MPC) |
| Autonomous control | Data residency location | | • Global network infrastructure |
| | ControllablIity throughout the lifecycle | Autonomous control over data collection | • Data Security Center (DSC)<br>• Log Tank Service (LTS)<br>• Cloud Trace Service (CTS)<br>• Cloud Bastion Host (CBH) |
| | | Autonomous control over data migration and transmission | • Cloud migration methodology: 12 steps in 7 phases<br>• Simple Message Notification<br>• Distributed Message Service<br>• Cloud Data Migration (CDM)<br>• SSL Certificate Manager (SCM)<br>• VPN<br>• Direct Connect<br>• Cloud Connect<br>• Data Express Service (DES)<br>• Migration Center (MgC) |
| | | Autonomous control over data storage | • DSC<br>• Data Encryption Workshop (DEW)<br>• Dedicated HSM<br>• Key Management Service (KMS)<br>• Key Pair Service (KPS)<br>• Cloud Secret Management Service (CSMS)<br>• Database Security Service (DBSS)<br>• Object Storage Service (OBS) |

| Principle | Capability | Sub-capability | Capability or Product |
|---|---|---|---|
| | | Autonomous control over data use | • Identity and Access Management (IAM)<br>• Application Trust Center (ATC)<br>• CBH<br>• DBSS<br>• API data security<br>• Digital watermarking<br>• Data masking |
| | | Autonomous control over data destruction | • Cloud Data Migration (CDM)<br>• CTS<br>• KMS |
| Transparency and visibility | Customer service response | | • Contractual commitment<br>• Response to data subjects' rights requests<br>• CTS<br>• LTS |
| | Response to regulatory requirements | | • Response to legal and regulatory requirements<br>• Judicial assistance |
| | Requirements for contractors | | • Contractor management mechanism |
| | Audit & certification | | • Certificates |

# 5 Building a Security Foundation to Ensure Data Security on the Cloud

The security protection of content data on the cloud relies on a secure and reliable cloud environment. Huawei Cloud has built a secure and reliable cloud platform infrastructure based on Huawei's more than 30 years of security experience and best practices in cloud security both within and outside China. It provides basic security protection capabilities for customers' content data on the cloud.

Huawei Cloud provides basic security protection capabilities for customers' content data (data at rest, data in transit, and data in use) on the cloud. Additionally, Huawei Cloud embeds routine security management and governance activities into relevant business processes and tools, ensuring consistent and effective implementation of security requirements and measures.

## 5.1 Key Protection

Huawei Cloud provides a secure, reliable, and easy-to-use key hosting service through the KMS in the DEW. KMS uses HSMs to protect keys and help customers create and manage keys. All keys are protected by root keys in HSMs to prevent key leakage.

- **KMS**

  KMS is a secure and easy-to-use key hosting service on the cloud. It uses HSMs to protect keys, and can be integrated with other Huawei Cloud services to protect data stored on these services. Customers can also use KMS to develop their own encryption applications. KMS interworks with numerous cloud-native services to offer native cloud encryption capabilities.

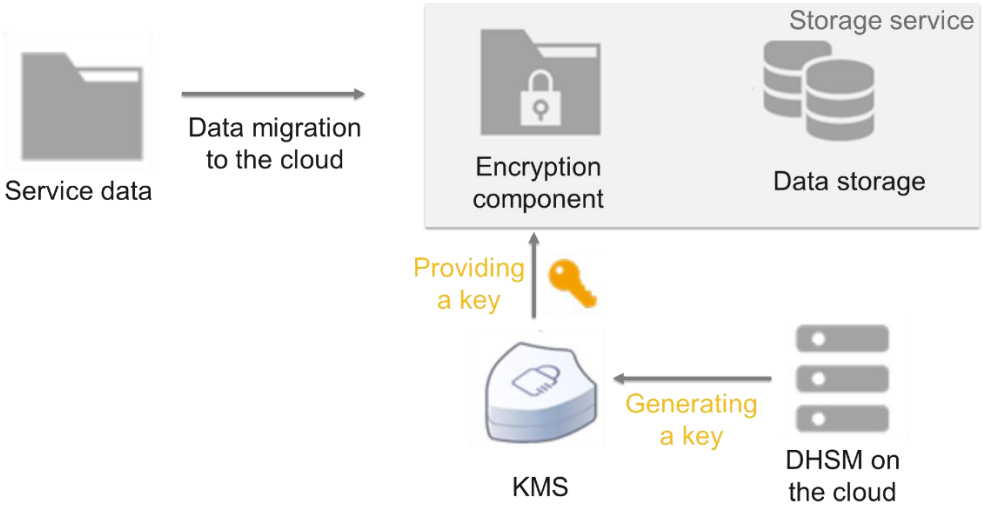
  KMS can be applied in many different service scenarios, including storage, big data, databases, and IoT scenarios. Both its software and hardware satisfy the requirements of Chinese cryptographic algorithms. KMS delivers 50,000 transactions per second (TPS) for a single customer, with API calling performance four times the industry average.

  KMS provides the following core functions:

  1. Key lifecycle management: includes creating, viewing, enabling, disabling, scheduling and canceling the deletion of customer master keys (CMKs), and modifying aliases and descriptions of CMKs.

2. Cloud service encryption: encrypts cloud storage services, such as OBS, EVS, IMS, SFS, RDS, DDS, and DWS.
3. Key rotation: Widely or repeatedly used keys are insecure. KMS key rotation ensures the security of encryption keys.

**Figure 5-1** KMS service architecture



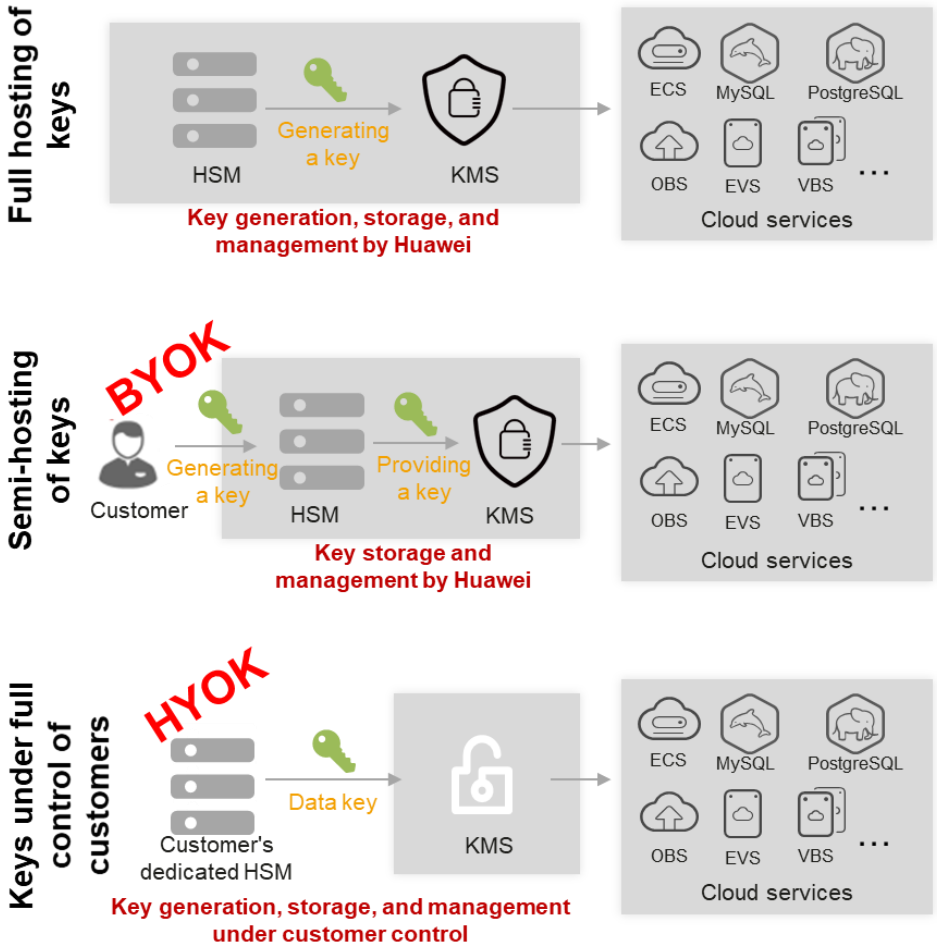

KMS provides three methods for customers to control their keys and meet different security requirements:

**Full hosting**: Keys are generated, stored, and managed on Huawei Cloud to minimize key management workloads. This method applies to small- and medium-sized enterprises and individual users.

**Semi hosting (Bring Your Own Key, BYOK)**: Customers generate keys and import them to Huawei Cloud, where the keys are stored and managed. The method is suitable for users whose keys are generated locally or by a third party, and it promotes autonomous control over key generation. It is applicable to governments and enterprises, including gaming and finance companies.

**Full control (Hold Your Own Key, HYOK)**: Customers control key generation, storage, and management by using dedicated HSMs provided by Huawei. This method is suitable for users who face strict supervision and store important and sensitive data on the cloud. It helps them maintain full control throughout the key lifecycle. It is applicable to banks, governments, and enterprises, including large multinational companies.

**Figure 5-2** Three service models of KMS




**Service resources**

- KMS

# 5.2 Security of Data at Rest

## 5.2.1 Data Reliability

Data reliability is a crucial area of focus for Huawei Cloud data security management. To ensure the stability and reliability of customer data, Huawei Cloud's storage products, such as EVS, databases, and OBS, have adopted technical measures to offer high-reliability data storage capabilities to customers. The following table lists some of the examples.

**Table 5-1** Huawei Cloud service reliability

| Storage Type | Reliability Assurance |
| --- | --- |
| Elastic Volume Service (EVS) | EVS provides a multi-copy (three-copy) data redundancy mechanism, storing data redundancies in multiple physical locations to ensure data reliability and consistency. It adopts synchronized data read and write mechanisms for all copies. It can automatically rectify hardware faults in the backend and quickly rebuild data. The data durability reaches 99.9999999%. EVS backup and restoration are implemented using CBR, and EVS instances can be created through backup. |
| Cloud Backup and Recovery (CBR) | Backup data is stored across data centers, with data durability up to 99.999999999%.<br>CBR allows you to create multi-AZ vaults to store the backup data to multiple AZs of a Region. When an AZ is unavailable, data can still be accessed from other AZs. CBR applies to scenarios where high reliability is required. |
| OBS | Data durability reaches up to 99.9999999999%. The Service Availability Rate of the Standard storage in a single AZ per Service Cycle is not lower than 99.99%; and that of the Standard storage across three AZs per Service Cycle is not lower than 99.995%.<br>Data check: OBS uses the hash algorithm to verify data consistency before and after storage to ensure that the stored data is the uploaded data.<br>Slice redundancy: Data slices are stored redundantly in different disks, allowing the system to verify data consistency and automatically recover compromised data in the backend. |
| Scalable File Service (SFS) | With high-reliability network and redundancy design of service nodes, the data durability of SFS reaches up to 99.9999999%, and the service availability reaches 99.95%. File storage backup and restoration are achieved through CBR. |
| Relational Database Service (RDS) | RDS uses the hot standby architecture, offering two backup and restoration methods: automated backups and snapshots. RDS automatically backs up full data and incrementally backs up transaction logs every five minutes. This allows tenants to restore data to any point in time ahead of the last incremental backup.<br>A failover upon fault occurrence takes only one minute. Data is automatically backed up every day and uploaded to OBS buckets. Backup files are stored for 732 days. One-click restoration is supported. |
| Image Management Service (IMS) | Private images are stored in multiple copies, achieving up to 99.999999999% data durability. |

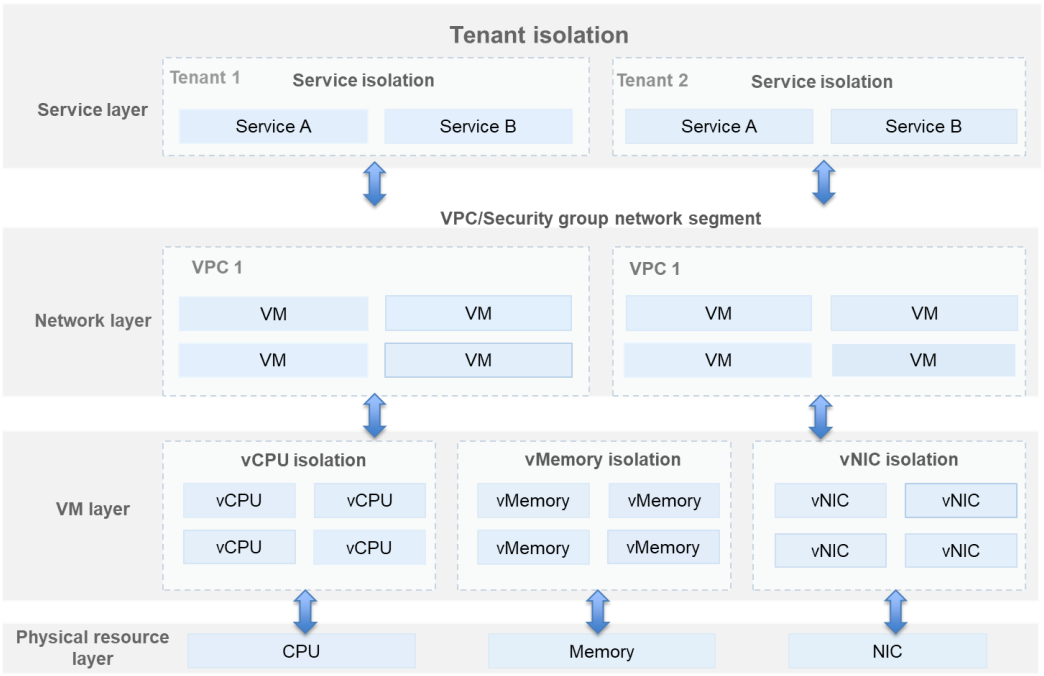
The service level agreement (SLA) of Huawei Cloud clearly outlines the service availability for products such as EVS, databases, and OBS. If the service availability

falls below the promised standards, customers will receive compensation as specified in the agreement.

## 5.2.2 Data Isolation

Huawei Cloud designs data isolation at the physical resource layer, VM layer, network layer, and service layer, achieving comprehensive data isolation from the underlying physical storage and compute resources to the top-layer service resources. This approach prevents unauthorized access to user data and ensures comprehensive data security and controllability in the cloud.

**Figure 5-3** Huawei Cloud data isolation solution




- **Virtual compute resource isolation**

  Huawei Cloud abstracts underlying physical compute resources, such as CPUs, memory, and I/O devices, into virtualized compute resources, such as vCPUs, virtual memory, and virtual I/O devices. The virtualization platform controls the access of VMs to virtual compute resources, allowing each VM to access only its own compute resources, ensuring data security. Examples of virtual compute resource isolation are as follows:

  1. **CPU isolation:** It mainly refers to the isolation between the virtualization platform and VMs, permission allocation of VMs, and isolation between VMs. CPU isolation is implemented by switching between the root and non-root modes, allocating running rights in each running mode, and allocating and switching virtual compute resources in the form of vCPUs. By using CPU isolation, the UVP controls the access rights of VMs to physical devices and virtual running environments. In this way, information and resources can be isolated between the virtualization platform and VMs and between different VMs. To be specific, a VM cannot access information and resources of the virtualization platform or other VMs.

2. **Memory isolation:** The virtualization platform also provides memory resources for VMs and ensures that each VM can access only its own memory. To achieve this goal, the platform ensures that memory space used by each VM has one-to-one mapping with the physical memory space. The VM accesses memory through address translation at the virtualization layer. This ensures that each VM can access only the physical memory allocated to it and cannot access the memory used by other VMs or by the virtualization platform.
3. **I/O isolation**: The virtualization platform provides virtual I/O devices for VMs, including disks, NICs, mouse devices, and keyboards. It also provides independent devices for each VM to prevent information leakage caused by device sharing between multiple VMs. Each virtual disk corresponds to an image file or logical volume on the virtualization platform. The platform ensures that only one virtual disk of a VM is associated with an image file. This ensures one-to-one mappings between virtual devices used by VMs and I/O managed objects on the virtualization platform and ensures that VMs cannot access I/O devices of other VMs, thereby isolating I/O paths.

- **Network isolation**

  Huawei Cloud isolates the data in the cloud using a Virtual Private Cloud (VPC). The VPC uses a network isolation technology to achieve isolation between tenants at the Layer 3 network, allowing tenants to fully control the construction and configuration of their virtual networks. A VPC can be connected with a tenant's traditional data center through the VPN or Direct Connect for application and data migration to the cloud. The ACLs and security group functions of the VPC can be configured as required for finer-grained network isolation.

  A VPC can be used to create a private network environment for customers. A VPC can be partitioned into multiple zones, such as DMZ, service, and data zones, and security groups can be used to isolate IP address ranges, subnets, and VMs within the VPC. Customers can employ relevant network access control policies of the VPC and security groups to ensure the security of network border access.

- **Service isolation**

  By default, different VPCs cannot communicate with each other, which achieves data isolation between customers and significantly reduces the risk of data breaches between different customers. Furthermore, customers can freely configure network isolation policies for subnets and security groups within a VPC. By deploying different storage and database service instances, such as OBS and RDS instances, into different security groups, storage resources within the VPC can be isolated, reducing the risk of data breaches caused by arbitrary communication between storage services.

## 5.2.3 Storage Encryption

With reference to industry best practices, Huawei Cloud has developed and implemented cryptographic algorithm application specifications, clearly defining the encryption levels and methods. In compliance with the specifications, Huawei Cloud uses the Advanced Encryption Standard (AES) algorithm to encrypt the data stored in cloud infrastructure, effectively protecting data security on the cloud platform. Regarding key management, the Huawei Cloud key security specifications describe how keys shall be managed throughout their lifecycles, including generation, transmission, use, storage, update, and destruction.

### 5.2.4 Secure Data Destruction

When customer data is destructed on Huawei Cloud, the data and all its copies are cleared. After a customer confirms data deletion, Huawei Cloud first deletes the index relationship between the customer and the data. Then, Huawei Cloud zeroes out the storage resources involved, such as memory, block storage space, OBS and SFS. This ensures that deleted data and related information cannot be restored or leaked after the storage resources are reallocated.

In terms of physical medium destruction, Huawei Cloud also implements a comprehensive storage media disposal mechanism based on industry standards to ensure data security at the end of the data center media lifecycle. For example, it follows the NIST SP 800-88 standard for handling storage media. For storage media that need to be reused, data is securely deleted using methods such as random number overwriting and cryptographic erasure. For storage media that do not need to be reused, physical destruction methods, such as degaussing and physical destruction, are employed.

### 5.2.5 Access Control

Huawei Cloud implements standardized and normalized access control, authorizing O&M personnel to perform RBAC and strict SoD management. O&M personnel cannot access customer data without customer authorization.

O&M personnel access O&M environments using two-factor authentication via a bastion host. After O&M operations, the passwords for logging in to the environments are reclaimed and periodically updated by the bastion host, ensuring that O&M personnel neither need nor can obtain the passwords.

Additionally, Huawei Cloud has established a centralized and comprehensive log audit system. All internal O&M operations are collected and documented by the system. Huawei Cloud regularly monitors and audits various activities in the O&M process, and any abnormal operations are promptly alerted and blocked. Violators will be punished according to relevant regulations.

## 5.3 Security of Data in Transit

### 5.3.1 Transmission Encryption

On Huawei Cloud, when data is transmitted from servers to clients or between servers through public information channels, the data is protected using the following methods:

- **VPN**

  VPN is used to establish a secure encrypted communications tunnel that meets industry standards between a remote network and a VPC, seamlessly extending the existing DC to Huawei Cloud and providing end-to-end confidentiality protection for tenant data during transmission. With the communications tunnel established between a traditional DC and a VPC through the VPN, tenants can easily use Huawei Cloud's resources, such as cloud servers and block storage. Applications are migrated to the cloud and additional web servers are started to increase the network computing capacity, which enables a hybrid cloud architecture and reduces risks of unauthorized dissemination of core enterprise data.

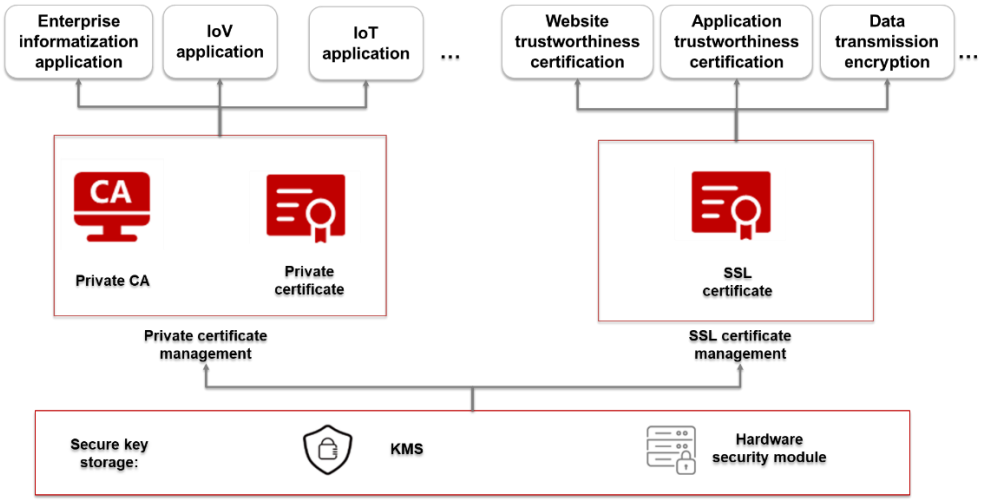
Currently, Huawei Cloud encrypts data transmissions using the hardware-assisted Internet Key Exchange (IKE) and Internet Protocol Security (IPsec) VPN to ensure transmission security.

- **Application Layer TLS and Cloud Certificate Manager (CCM)**

  Huawei Cloud supports REST- and Highway-based data transmission methods. Both methods support encrypted transmission using newer TLS versions and also support identity authentication for target websites based on X.509 certificates.

  CCM is a service for large-scale certificate issuance and lifecycle management on the cloud, providing SSL certificate management and private certificate management services. It provides certificates encrypted with mainstream cryptographic algorithms (RSA and ECC) and certificates encrypted with SM2 and relevant cryptographic algorithms. CCM can automatically update and rotate multi-year SSL certificates applied to other services. This frees you from manual workloads and cuts your time and labor costs. It provides great flexibility through abundant APIs, meeting diverse service requirements. Additionally, it uses KMS and HSMs to provide stable and reliable security protection for keys.

**Figure 5-4** CCM service architecture




**CCM provides the following core functions:**

1. Certificate lifecycle management: Customers can request, issue, query, and revoke public SSL certificates and private certificates and manage tens of millions of certificates.
2. Private CA hosting: Customers can easily manage CAs on Huawei Cloud on a pay-per-use basis, without the need to build or maintain complex CA infrastructure.
3. One-click SSL certificate deployment: Certificates can be deployed to mainstream cloud products in one-click mode and automatically updated and rotated upon expiration.

## 5.3.2 Stable and Reliable Transmission

Huawei Cloud not only ensures the security of data transmission on the cloud, but also provides customers with high-performance, high-reliability, and low-latency network transmission. Huawei Cloud provides multi-link disaster recovery (DR) for

customers by allowing them to access their Virtual Private Cloud (VPCs) on the cloud via multiple dedicated connections from different carriers. When one link fails or the entire network of a carrier fails, traffic automatically fails over to another link provided by another carrier, ensuring service continuity.

- **Direct Connect**

  Direct Connect is a high-speed, low-latency, stable, and secure dedicated network connection that connects a local data center to a VPC on Huawei Cloud. It extends Huawei Cloud services and existing IT facilities to build a flexible, scalable hybrid cloud computing environment. Direct Connect provides dedicated channels, safeguarding service security. It uses a dedicated private channel to connect to a Huawei Cloud VPC, ensuring network isolation and high security.

**Service resources**

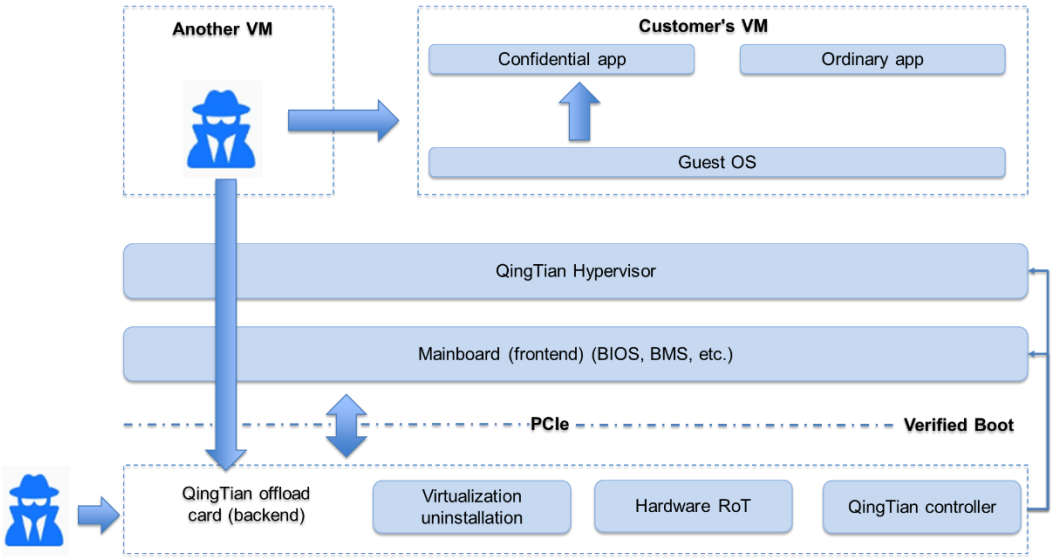
- **VPN**
- **CCM**
- **Direct Connect**

# 5.4 Security of Data in Use

## 5.4.1 Confidential Computing

To ensure the security and trustworthiness of customer data procesing on the cloud, Huawei Cloud has developed the QingTian confidential computing platform based on the trustworthiness design principles and the characteristics of cloud platform infrastructure. This platform provides customers with high-performance ECS instances that are highly secure, strongly isolated, and cost-effective. The following figure illustrates the platform's security conceptual model.

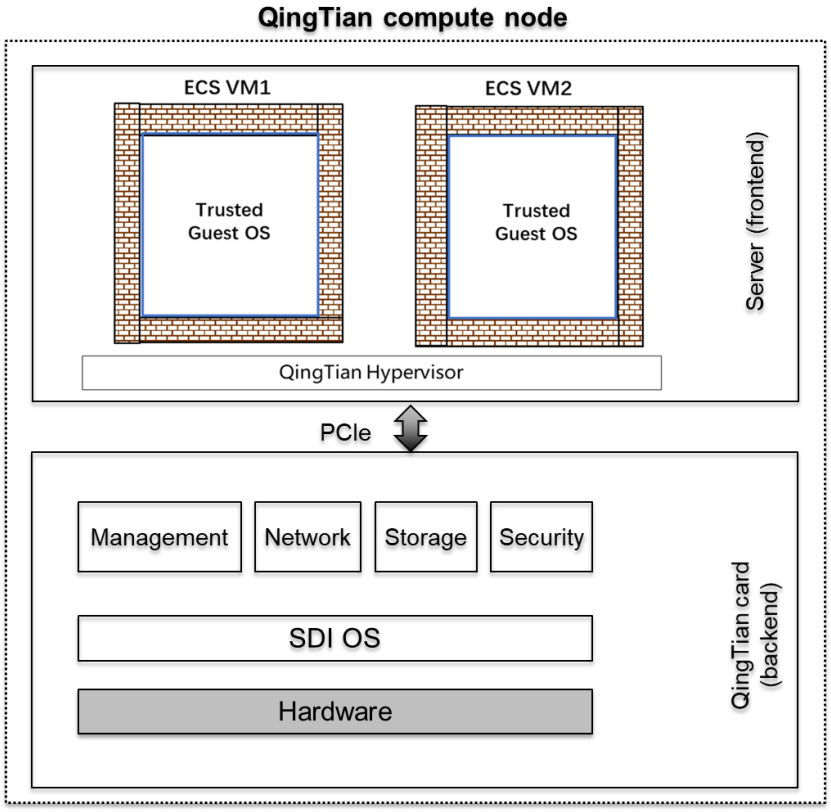
**Figure 5-5** QingTian security conceptual model



The QingTian virtualization platform is designed to provide significantly enhanced security control and privacy protection capabilities. In terms of confidentiality and integrity protection, the platform builds the minimum trusted computing base (TCB) based on the following design principles: reactive connection design, unidirectional access control, minimized attack surface, frontend and backend hardware isolation, hardware identity proof and trust, hardware key protection and end-to-end encryption/decryption, mandatory secure boot, and integrity verification.

**Isolation dimension 1: Customer's application code and data are isolated from O&M and cloud system software of cloud service providers**

**Figure 5-6** Customers' application code and data are isolated from O&M personnel and cloud system software of cloud service providers




- **No access from O&M personnel:** To ensure mandatory isolation between customer instances and between customer instances and cloud infrastructure, QingTian Hypervisor does not provide any mechanism for remote login. This can mitigate attacks such as memory dumping. Internal O&M personnel typically can only utilize O&M APIs for remote diagnostics and are unable to log in to the frontend Hypervisor or access memory data of customer instances on the frontend servers.
- **Escape prevention:** The QingTian system is a frontend and backend separated VMM architecture, where the frontend and backend are physically isolated based on the PCIe bus. Huawei Cloud adheres to the minimum TCB design principle. The frontend Hypervisor is minimally designed, with no network protocol stack, local storage, or SSH management tools. The frontend Hypervisor creates and isolates customer instances based on hardware

virtualization, while the backend SDI card uses SR-IOV passthrough for access to VM instances without using management software. Compared with traditional virtualization management systems, QingTian Hypervisor has less than 1% code, indicating that the software security risks in the QingTian system are substantially decreased.

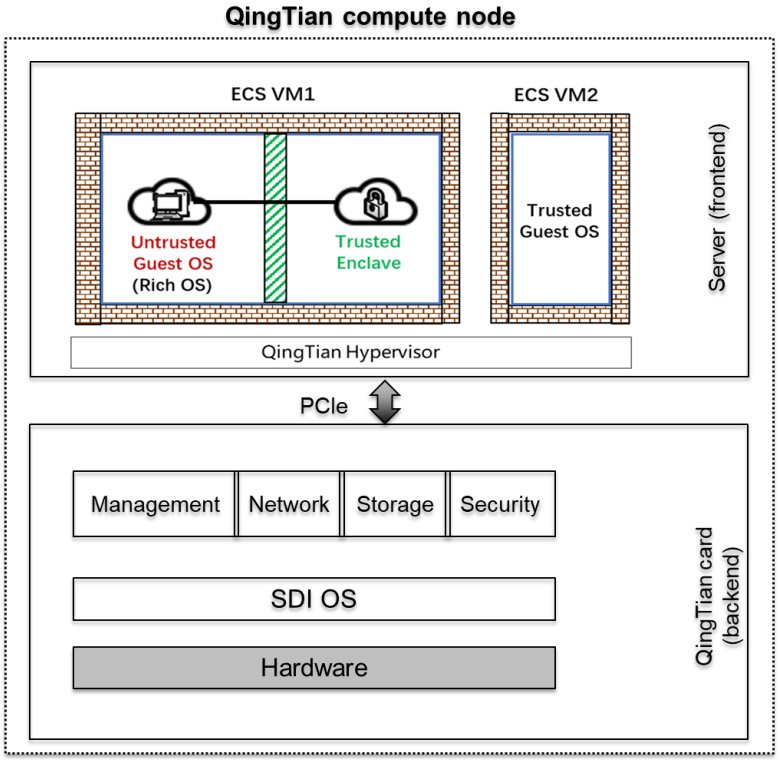
- **Anti-tampering at the system level:** Huawei Cloud uses mandatory secure boot in the QingTian system. The backend SDI card initiates secure boot and then verifies the integrity of the system firmware and frontend Hypervisor image signature. Upon successful verification, the frontend Hypervisor is started. For customers' ECS VMs, Huawei Cloud allows customers to enable secure boot in compliance with the UEFI Secure Boot standard when they create VMs. It also allows customers to enable QingTian vTPM (compliant with TPM 2.0 specifications) to implement trusted boot and remote attestation.
- **Defense against physical attacks:** Huawei Cloud enables volume encryption and VPC encryption on QingTian cards, and uses hardware to protect keys. Customers have full control over the use of data keys, and QingTian cards encrypt data as it leaves compute nodes and decrypt it as it enters.

In this isolation dimension, Huawei Cloud also provides tenant-exclusive BMS bare-metal instances based on QingTian cards. For bare-metal instances, no QingTian Hypervisor is running on servers. Customers can exclusively access the underlying mainboard system and use related hardware features (such as Intel VT and ARM TrustZone) to satisfy their mandatory isolation requirements.

**Isolation dimension 2: Customers' application code and data are isolated from their O&M personnel and low-trustworthiness software**

Based on the security design of isolation dimension 1, Huawei Cloud provides QingTian Enclave in ECS instances to isolate customers' application code and data from their O&M personnel and low-trustworthiness software. QingTian Enclave is an isolated runtime environment initiated within the customer's ECS instance. It is connected to the instance via a unique vsock channel. QingTian Encalve and ECS instances are isolated through hardware virtualization. QingTian Enclave not only inherits the security protection capabilities of ECS instances, but also provides a highly isolated computing environment using the following methods:

**Figure 5-7** Customers' application code and data are isolated from their O&M personnel and low-trustworthiness software




- **Enclave's minimal TCB:** Ordinary customer instances typically have a substantial TCB (such as Rich OS), which often results in a large security attack surface. QingTian Enclave is not designed to minimize the attack surface of the Rich OS but to thoroughly keep the Rich OS outside its trust boundary. Therefore, security threats to the Rich OS will not compromise the applications and data within Enclave. To minimize its attack surface, QingTian Enclave does not support IP network access, persistent storage, or SSH interactive access.
- **Isolation from customers' untrusted system software:** QingTian Enclave is isolated from customers' main ECS instances through hardware virtualization. There is no shared physical memory or CPU core between QingTian Enclave and ECS instances. QingTian Enclave is connected to the main ECS instance via a unique vsock channel protected by Hypervisor. All software systems running on the main instance cannot access the code and data in QingTian Enclave.
- **Protection from customers' untrusted O&M personnel:** As Huawei Cloud places customers' main instances (such as Rich OS) outside the trust boundary of QingTian Enclave, O&M personnel (including root or administrator users) who log in to the instances are denied access to the code and data in QingTian Enclave.
- **QingTian Enclave integrity protection and attestation:** Upon starting QingTian Enclave, QingTian Hypervisor verifies the digital signature of its image, measures the QingTian Enclave image file and its digitally signed public key certificate, and stores the measurement results in the QingTian security module (QTSM). The QTSM is a dedicated security module for managing trusted measurement results in cloud scenarios.

- **High usability and compatibility:** Huawei Cloud designs QingTian Enclave as a developer-friendly platform. Developers can easily develop QingTian Enclave applications without the need to understand CPU microarchitecture and advanced cryptography. Currently, QingTian Enclave supports both x86 and ARM architectures, allowing developers to use their familiar language frameworks and directly build QingTian Enclave images based on container images.
- **Cloud service integration:** The QingTian system supports cryptographic attestation for QingTian Enclave identities and trusted measurement results. QingTian Enclave applications use the Attestation protocol to verify their Enclave identities and foster trust with external services. Huawei Cloud KMS and IAM inherently support QingTian Enclave attestation. QingTian Enclave application developers can utilize the open-source Enclave SDK to access KMS APIs to obtain data encryption/decryption keys or secure random numbers and ensure end-to-end security. The customer administrator can implement conditional access control based on attestation for KMS APIs, using either the preset IAM authorization policy or the guardrail policy.

QingTian Enclave enables customers to create highly isolated and enhanced computing environments within ECS VMs. Recently, it also enables them to classify their system components into functions with different trust levels. This security feature has been favored by many cloud customers since its launch. Typical security applications developed by customers based on QingTian Enclave include the virtual HSM (vHSM), CSMS, Web3 Digital Wallet, confidential AI application, secure MPC, secure key negotiation, and end-to-end encryption. Huawei Cloud is building a wide range of open source QingTian Enclave tools (such as qproxy) and security solutions (such as confidential container), aiming to help more customers migrate their application code and build systems to the cloud without requiring any reconstruction efforts.

## 5.4.2 Homomorphic Encryption

Huawei Cloud uses homomorphic encryption to encrypt sensitive customer data on the cloud. During data processing, the original content of the data remains inaccessible to anyone, ensuring the security of sensitive data. Customers can encrypt sensitive data and then send the encrypted data to the cloud for processing and subsequently decrypt the results with secret keys. In sensitive data processing scenarios, homomorphic encryption enables Huawei Cloud to perform computation on ciphertext without requiring decryption from the key holder. This approach enhances data security while reducing communication costs.

## 5.4.3 Multi-Party Computation

Based on MPC, Huawei Cloud can perform joint computation and analysis on multi-party data across organizations or industries while protecting the security of customers' important data and privacy data. In this way, a mutual trust alliance can be established among multiple parties in a distributed and mutually untrusted environment, enabling multi-party data analysis and joint learning modeling across organizations or industries. MPC enables multi-party data convergent analysis while ensuring the confidentiality of customers' original data, thereby unlocking greater value of data utilization.

# 6 Providing Full-Stack Security Services to Enable Customers to Control Their Data on the Cloud

## 6.1 Data Residency Location

Huawei Cloud continues to expand data centers and acceleration networks around the globe. With cloud-network synergy, it strives to connect people, things, and applications, provide one global network with consistent experience, and enable efficient distribution and processing of information flows so that cloud services can be quickly delivered to where they are needed. Currently, infrastructure is deployed globally, covering more than 170 countries and areas, with almost 100 AZs under operations in over 30 Regions (both self-operated and jointly-operated ones) in Asia Pacific, Latin America, Africa, Europe, Middle East, and more. Huawei Cloud has launched over 220 cloud services and over 210 solutions to address different requirements.

Thanks to the extensive infrastructure network that Huawei Cloud has built globally, customers can deploy applications and services in the most suitable geographic locations to meet their business requirements. With the official website of Huawei Cloud, customers can gain a comprehensive understanding of global data center deployment, including locations, sizes, technical specifications, and SLAs of different data centers. Such transparency not only enhances customers' trust in the locations where their data is stored but also provides enterprises with necessary information to make informed decisions based on their business expansion strategies, legal and regulatory requirements, and performance optimization needs.

With this information, customers can clearly understand which services are available in specific Regions and which services might be used across Regions. It is particularly important for enterprises with specific compliance requirements, such as certain industries that mandate data be stored within specific countries or areas. Additionally, for applications that require high performance and low latency, choosing a data center close to the user base is crucial. Therefore, the detailed information provided by Huawei Cloud enables customers to better plan their IT infrastructure, ensuring alignment with both business objectives and technical requirements.

# 6.2 ControllabIlity Throughout the Lifecycle

Centering on data, Huawei Cloud develops full-stack data security services covering the entire data lifecycle. Critical data is protected with in-depth defense mechanisms. Full-stack encryption, customer-held keys, customer-authorized remote O&M, and other measures are adopted to ensure that customers maintain autonomous control over their data security.

## 6.2.1 Autonomous Control over Data Collection

### 6.2.1.1 Data Collection

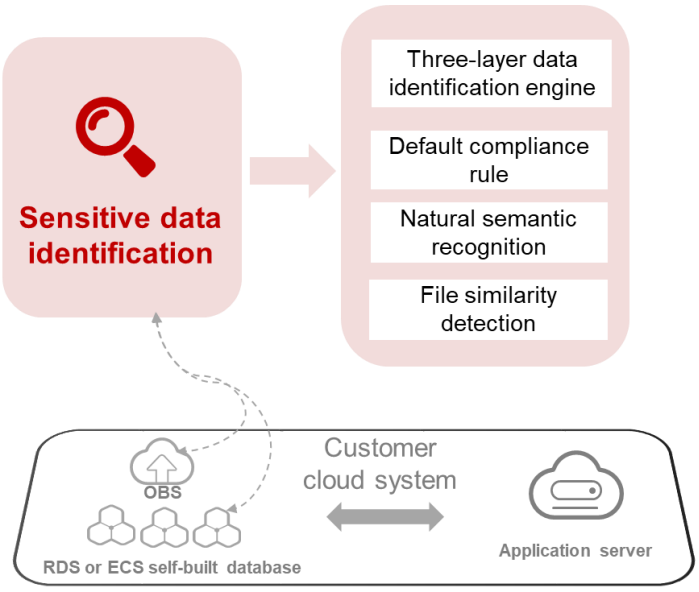
At the application layer, customers can use LTS to collect log data from both hosts and cloud services. The collected log data is displayed on the LTS console in a clear and orderly manner. Huawei Cloud offers CTS and CBH for audits, allowing the collection of all operations and changes performed in cloud environments. This data can be used to support security analysis, compliance audits, resource tracking, and fault location.

### 6.2.1.2 Data Identification, Classification, and Categorization

- **DSC**

  Customers can use Huawei Cloud DSC to classify and categorize their data. DSC provides built-in and user-defined sensitive data scanning rules to identify sensitive information for classification and categorization. Customers can customize sensitive data categories, identification rules, and levels based on their business needs, automating sensitive data recognition and data classification & categorization.

**Figure 6-1** Sensitive data identification by DSC




DSC can help customers discover privacy data from hundreds of millions of files and rapidly identify sensitive fields from terabytes of data. It builds an automated three-layer data identification engine to present the overall risks as soon as the

data is generated. It supports 200 data formats, including both structured and unstructured data, ensuring comprehensive scenario coverage.

**Service Resources**

- **LTS**
- **CTS**
- **CBH**
- **DSC**

## 6.2.2 Autonomous Control over Data Transmission

Data transmission refers to the transfer of data over a network from a data source to a destination. Huawei Cloud enables customers to have autonomous control over data migration, data transmission, and transmission encryption through its cloud services and cloud migration practices.

### 6.2.2.1 Autonomous Control over Data Migration

Huawei Cloud has developed a "12 steps in 7 phases" cloud migration methodology that covers all scenarios and stages of data migration, both into and out of the cloud. This methodology is built based on successful cloud migration practices and extensive experience in helping a large number of customers. To ensure data security during cloud migration, Huawei Cloud provides various security tools, professional services, and solutions to help customers securely migrate their applications and data to the cloud and maintain continuous security of their cloud services. During migration, MgC can be used to transfer and modernize applications and data, achieving cost effectiveness and fostering innovation.

### 6.2.2.2 Autonomous Control over Data Transmission

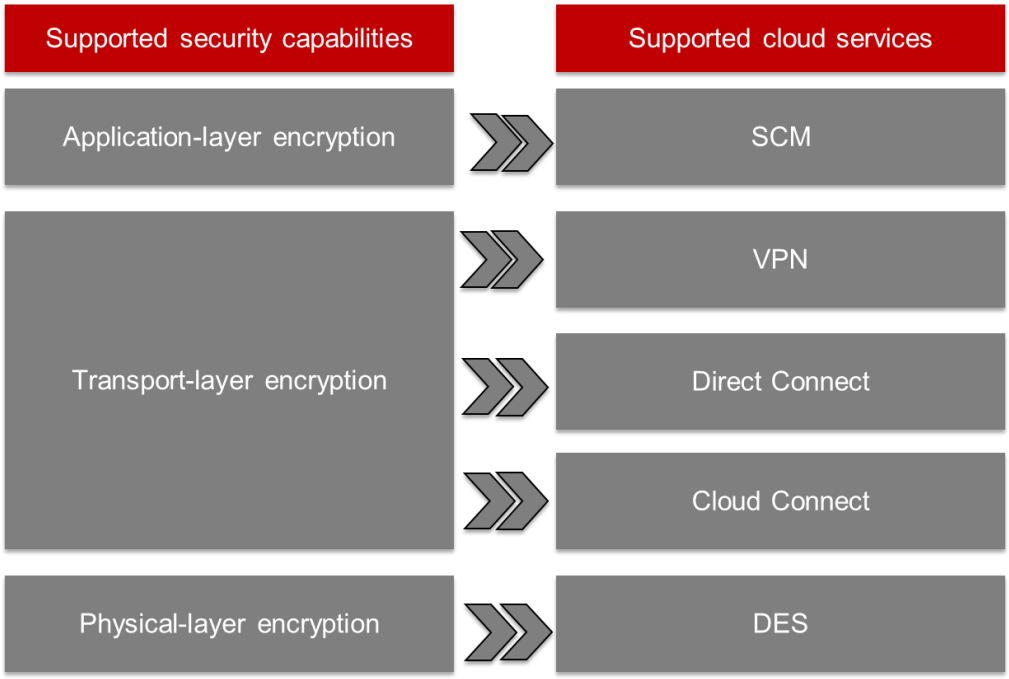
Huawei Cloud offers services to help customers secure data transmission in cloud environments. If a customer's business changes, they can control data transmission by either stopping the use of relevant services or selecting other transmission services, such as SMN, DMS, and CDM. Huawei Cloud provides necessary security capabilities to assist customers in enhancing the security of data transmission when they use these services.

### 6.2.2.3 Autonomous Control over Transmission Encryption

Huawei Cloud offers multiple transmission encryption solutions, including SCM, VPN, Direct Connect, Cloud Connect, and DES, for different scenarios at the application, transport, and physical layers. Customers can choose their own transmission encryption mechanisms for specific scenarios to ensure secure data transmission.

Huawei Cloud recommends that customers encrypt data in transit to ensure its security.

**Figure 6-2** Huawei Cloud's data transmission security capabilities




- **SCM**

  When customers provide web services over the Internet, they can use SCM. They can also apply for and configure certificates for the websites to implement trusted identity authentication and secure data transmission through encryption protocols.

- **VPN**

  For customers with hybrid cloud deployment and global business presence, Huawei Cloud provides services such as VPN, Direct Connect, Cloud Connect, to achieve interconnectivity and secure data transmission between different Regions. VPN uses Huawei's professional equipment and creates a virtual private network over the Internet based on the IKE and IPsec protocols. It builds stable and reliable encrypted transmission channels between the local data center and Huawei Cloud VPC, as well as between VPCs in different Huawei Cloud Regions.

- **Direct Connect**

  Direct Connect leverages various types of dedicated line networks provided by carriers to establish a dedicated encrypted transmission channel between the local data center and Huawei Cloud VPC. Each customer's dedicated line is physically isolated from others, meeting higher requirements for security and stability.

- **Cloud Connect**

  Cloud Connect is a one-stop cloud connection network service built on Huawei's years of global IT operations experience and network resources in many countries and areas. It can quickly establish private communications networks between multiple local data centers and multiple VPCs, supporting interconnection across VPCs on different clouds and greatly improving the security and speed of customers' global service expansion.

- **DES**

  DES is a massive data transmission solution offered by Huawei Cloud. Users can utilize Teleport high-performance storage devices or hard disks to physically transport data to Huawei Cloud in a secure way. The Teleport device comes with AES-256 full-disk encryption, and customers can manage their keys by themselves. All data remains encrypted throughout the transmission process, effectively ensuring the security of data in transit.

**Service Resources**

- **SCM**
- **VPN**
- **Direct Connect**
- **Cloud Connect**
- **DES**
- **MgC**

## 6.2.3 Autonomous Control over Cross-Border Data Transfers

Customers may need to transfer cloud data across borders for business purposes when using Huawei Cloud services. In this context, they need to consider applicable laws and regulations, such as the EU General Data Protection Regulation (GDPR), Data Security Law of the People's Republic of China, Personal Information Protection Law of the People's Republic of China, Measures on the Security Assessment of Cross-Border Data Transfers, and Regulations on Promoting and Regulating Cross-Border Data Flows. Relevant laws and regulations may outline specific compliance requirements for cross-border transfers of specific categories of data, and therefore customers need to identify such requirements for effective management.

Huawei Cloud ensures secure and compliant cross-border data transfers by using different measures, including gaining insights into laws/regulations, reviewing cross-border data transfer scenarios, assessing cross-border transfer risks, adopting compliance measures, and conducting regular evaluation and review. Huawei Cloud takes into account local legal and regulatory requirements for cross-border data transfers in countries and areas where it operates. For details, see **Trust Center**.

- China

  For Chinese multinational companies or companies going global, if important data needs to be transferred out of China, security assessments and declaration of cross-border data transfers must be conducted in accordance with relevant Chinese laws and regulations. For cross-border transfers of personal information, companies must comply with legal/regulatory requirements based on the type and scale of the data. This includes applying for cross-border data transfer security assessments, entering into standard contracts on cross-border transfers of personal information, or obtaining personal information protection certifications.

  Additionally, companies shall confirm the responsibilities and obligations of the receiving party abroad and check whether they have necessary management and technical measures and capabilities. This is to prevent potential risks to national security, public interests, and legitimate rights and interests of individuals or organizations.

- EU

In EU cross-border data transfer scenarios, companies can conduct a data protection impact assessment (DPIA) to ensure that data transfers do not pose risks to the privacy and security of data subjects. Companies can ensure compliance of cross-border personal data transfers by signing standard contract clauses (SCCs) or using other protection measures recognized by the European Commission.

## 6.2.4 Autonomous Control over Data Storage

Huawei Cloud provides customers with a variety of functions and services, including query for Region information of data centers, data storage of Region- and Global-level services, data storage security protection, data isolation, and disaster recovery and backup. These features help customers achieve autonomous control over data storage security. Specifically, they include:

### 6.2.4.1 Query for Region and Location Information of Data Centers

Customers can choose to deploy their own data in any Region. They can leverage Huawei Cloud services and tools to manage their data, including determining storage locations, protection methods, and access permissions. For instance, they can query Region information of their data centers to see if data residency location requirements are met.

### 6.2.4.2 Data Storage of Region- and Global-Level Services

Huawei Cloud services are deployed at the Region and Global levels. Customers can utilize the data storage pages of Region- and Global-level services to gain detailed location information about their data.

### 6.2.4.3 Data Storage Security Protection

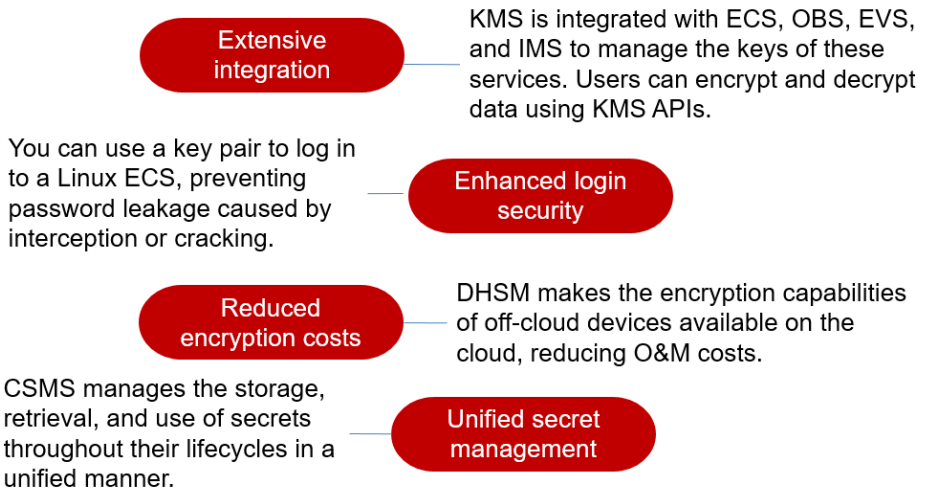
Huawei Cloud offers advanced data encryption technologies, allowing customers to choose their encryption algorithms and key management policies based on their security needs and compliance requirements. Huawei Cloud services, such as DEW, OBS, and SFS, provide data encryption (server-side encryption) and use high-strength algorithms to encrypt stored data.

- **DEW**

  DEW is a comprehensive cloud-based data encryption service that includes DHSM, KMS, and KPS, providing dedicated encryption, key management, key pair management, and other services. It aims to offer convenient, reliable, and efficient data encryption capabilities. DEW can be integrated with many other cloud services. Keys can be fully hosted, semi hosted, or fully controlled by users. Users can even use this service to develop their own encryption applications, controlling data security more flexibly.

  The following figure illustrates the core advantages of DEW.

**Figure 6-3** Core advantages of DEW

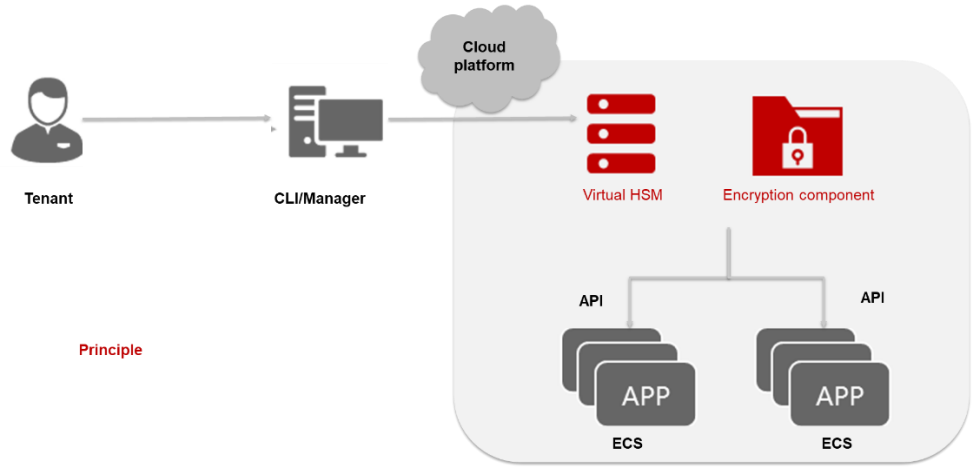



- **DHSM**

  DHSM is a cloud platform service that builds a virtualized cryptographic resource pool based on Cloud Hardware Security Modules (CHSMs), enabling unified scheduling and management of IT and cryptographic resources and providing Virtual Security Modules (VSMs) on demand. It enables tenants to migrate HSMs to the cloud, implement unified scheduling of cryptographic and IT resources, and automate management and maintenance. DHSM can handle operations such as encryption, decryption, signing, signature verification, key generation, and secure key storage, which helps protect the security and integrity of data on ECSs and meet regulatory compliance requirements. Tenants can also manage keys generated by dedicated encryption instances, and use diverse algorithms for data encryption and decryption. DHSM provides hardware encryption modules that meet the FIPS 140-2 Level 3 standard.

  DHSM is certified by a third-party organization. It ensures high-speed concurrent operations under different encryption protocols through its hardware cryptographic computing power.

**Figure 6-4** DHSM service architecture




The following table describes the key algorithms supported by DHSM.

**Table 6-1** Algorithms supported by DHSM

| Key Type | Algorithm Type |
|---|---|
| Symmetric keys | AES |
| | 3DES |
| | DES |
| | SM1 |
| | SM4 |
| Asymmetric keys | RSA_1024 |
| | RSA_2048 |
| | SM2 |
| Digest algorithms | SM3 |
| | SHA1 |
| | SHA256 |
| | SHA384 |

DHSM provides the following core functions:

1. Unified management of cryptographic and IT resources: supports the cloud platform's automated, unified scheduling and management of virtualized cryptographic resource pools, in conjunction with IT resources.
2. Dynamic elastic scaling: supports quick adjustment, replication, failover, and automated O&M.
3. Data encryption: supports both international and Chinese cryptography algorithms, covering both symmetric and asymmetric encryption.

- **KMS**

KMS provides secure, reliable, and easy-to-use key hosting services. It uses HSMs to protect CMKs, helping customers create and manage CMKs. All CMKs are protected by root keys in HSMs to prevent key leakage. KMS integrates with numerous cloud-native services to offer native encryption capabilities. Multiple cloud storage services can be encrypted, including OBS, EVS, IMS, SFS, RDS, DDS, and DWS.

The following table describes the algorithms supported by KMS.

**Table 6-2** Algorithms supported by KMS

| Key Type | Algorithm Type | Key Specifications |
|---|---|---|
| Symmetric keys | AES | AES_256 |
| | SM4 | SM4 |

| Key Type | Algorithm Type | Key Specifications |
|---|---|---|
| Asymmetric keys | RSA | RSA_2048<br>RSA_3072<br>RSA_4096 |
| | ECC | EC_P256<br>EC_P384 |
| | SM2 | SM2 |

- **KPS**

  KPS is a secure, reliable, and easy-to-use cloud service designed to help customers manage and protect SSH key pairs. It uses HSMs to generate true random numbers, which are then used to produce key pairs. It adopts a comprehensive, reliable key pair management solution to help users create, import, and manage SSH key pairs.

- **CSMS**

  CSMS is a secure, reliable, and easy-to-use cloud secret management service. Users or applications can use CSMS to create, retrieve, update, and delete secrets in a unified manner throughout the secret lifecycle. CSMS effectively prevents sensitive information leakage caused by hardcoding or plaintext configuration, and service risks that result from permission abuse. It also enables autonomous control over key management. CSMS has been interconnected with RDS and CCE to securely manage RDS and CCE secrets for customers.

  It can be used in scenarios such as human-machine, machine-machine, ECS, RDS, and self-built applications. APIs are provided for secret management and can be easily integrated into existing systems. The calling performance per API exceeds 500 TPS, meeting requirements in various scenarios.

  CSMS provides the following core functions:

  1. Secret encryption: Secrets are encrypted by KMS before storage. Encryption keys are generated and secured by HSMs that are certified by third parties.
  2. Secure secret retrieval: CSMS calls secret APIs instead of hard-coded secrets in applications so that secrets can be dynamically retrieved and managed programmatically for security.
  3. Centralized secret management: It is integrated with IAM to ensure that only authorized users can retrieve and modify secrets. It is integrated with CTS to monitor access to secrets. These services prevent unauthorized access to and leakage of sensitive information.

- **VBS**

  VBS creates online backup for individual or multiple EVSs without requiring shutdown or restart. It allows data to be restored to any backup point in scenarios such as virus intrusion, accidental deletion, and hardware and software failures. Backup data is encrypted and stored across data centers.

- **CSBS**

  CSBS creates consistent online backup for all EVSs on a cloud server without requiring shutdown. It allows data to be restored to any backup point in scenarios such as virus intrusion, accidental deletion, and hardware and

software failures. Backup data is stored in multiple data centers for protection against data-center-level failures.

- **SDRS**

  SDRS provides disaster recovery capabilities for ECS, EVS, and Dedicated Distributed Storage (DSS) services. It uses storage replication, data redundancy, cache acceleration, and other technologies to provide VM-level disaster recovery protection across AZs. When a production site fails, services can be quickly restored at the disaster recovery site with simple configuration, ensuring data reliability and service continuity.

**Service Resources**

- **DEW**
- **CBS**
- **VBS**
- **CSBS**
- **SDRS**
- **VPC**

## 6.2.5 Autonomous Control over Data Sharing

Data sharing refers to the exchange of data among users, customers, and contractors. Openness and sharing are the prerequisites for data convergence and mining, which helps eliminate information silos and unleash data value. To ensure secure data sharing and protect customers' rights and interest, customers are advised to strictly control data access and transmission. They can also use services related to data masking, digital watermarks, and secure MPC.

### 6.2.5.1 Data Masking

DSC supports static data masking and dynamic data masking. Customers can configure masking rules for specified data to implement static masking of sensitive data, and invoke APIs to implement dynamic data masking, preventing sensitive information leakage. During data sharing, customers can use different masking methods to mask sensitive data of different types. For example, sensitive personal data can be masked using character masking, and sensitive enterprise or device data can be masked by replacing keywords.

### 6.2.5.2 Digital Watermark

DSC provides digital watermarks that can be embedded into or extracted from documents, images, and JSON data. Digital watermarks are widely used in government departments, medical institutions, financial institutions, and scientific research institutions for copyright protection and source tracing.

1. Data copyright protection: In scenarios where important documents and images need to be provided to third parties, watermarks can be embedded into related data. In case of copyright disputes, digital watermarks can be used to identify the copyright owner.
2. Source tracing: When data is shared with an internal third party, user information is watermarked to identify the user and remind them to comply with security regulations. When a data breach occurs, digital watermarks can help organizations track the source and find the cause of the data breach.

# 6.2.6 Autonomous Control over Data Use

## 6.2.6.1 Access Control

Huawei Cloud always obtains the customer's explicit consent before accessing the customer's cloud data. Customers can also use IAM and CBH to set access control policies for different service scenarios, such as application access, O&M operations, and cloud resource access, preventing unauthorized access.

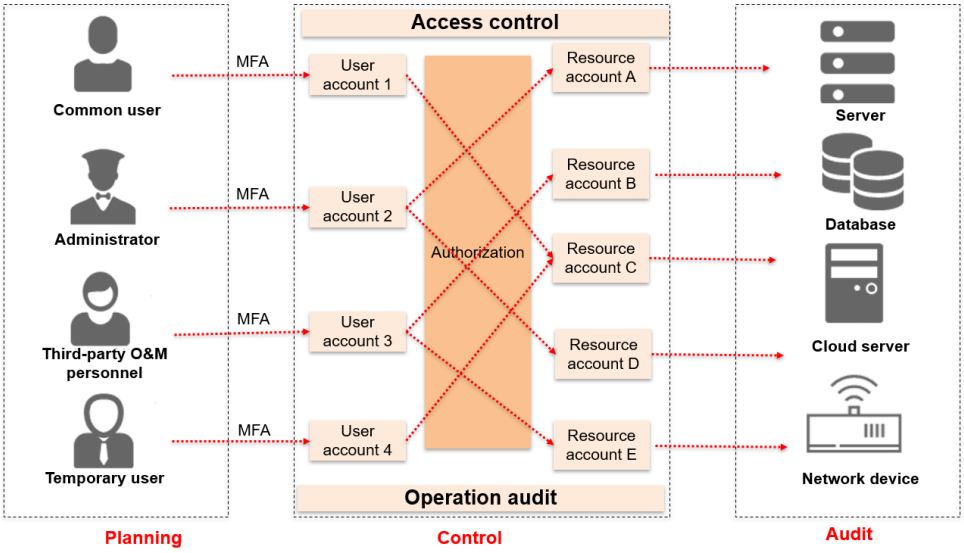
- **IAM**

  IAM provides customers with user account management, identity authentication, and fine-grained cloud resource access control that are suitable for enterprise users. It provides the MFA function to improve the security of account login and important operations. It also supports the digital signature and timestamp mechanisms to prevent API requests from being tampered with and to protect against replay attacks. It supports federated identity authentication, allowing customers to access Huawei Cloud resources after being authenticated by the existing account management system.

- **CBH**

  Malicious operations or misoperations by system O&M personnel may cause greater damage to the system than those performed by common users, as O&M personnel usually have higher permissions and are more likely to access underlying data than others. Therefore, Huawei Cloud recommends that customers use CBH to manage and control O&M activities. CBH provides one-stop account management, asset management, access control, and operation audit functions based on Huawei Cloud's years of experience in security O&M. CBH supports MFA to ensure remote login security, facilitating customers in O&M control and compliance audit.

**Figure 6-5** CBH service architecture



CBH provides the following core functions:

1. User management: user management, role management, MFA, and access policy
2. Resource management: password hosting, password change policy, O&M authorization, and application release
3. Access control: single sign-on (SSO), command interception, secondary authorization, and service ticket management
4. Operation audit: real-time monitoring, operation playback, command audit, and report analysis

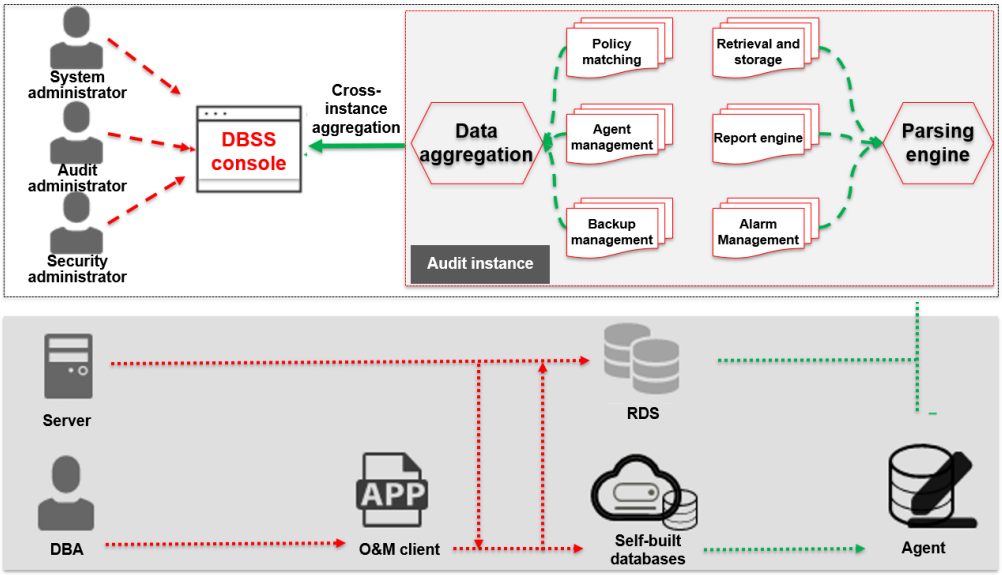
## 6.2.6.2 Data Masking and Data Breach Prevention

- **DBSS — Database security audit**

  The database security audit service is deployed in bypass mode, auditing user operations without affecting database performance. It records user access to the database in real time, generates fine-grained audit reports, sends real-time alarms for risky operations and attack behaviors. In addition, the database security audit service generates compliance reports that meet data security standards (such as Sarbanes-Oxley Act) to locate internal violations and improper operations, thereby ensuring data asset security.

  The database security audit service is easy to use and is deployed in bypass mode for safer O&M. With the database security audit service, RDS databases can be audited in agent-free mode. Full audit can be enabled on the data source side. SSL encrypted connections can be audited. The database security audit service provides comprehensive SQL parsing and precise protocol analysis Chinese databases are supported. The database security audit service meets the database audit requirements of Multi-Level Protection Scheme (MLPS) Level-3 and complies with laws and regulations such as China's Cybersecurity Law and Sarbanes-Oxley Act (SOX).

**Figure 6-6** DBSS capability overview (1)



DBSS provides the following core functions:

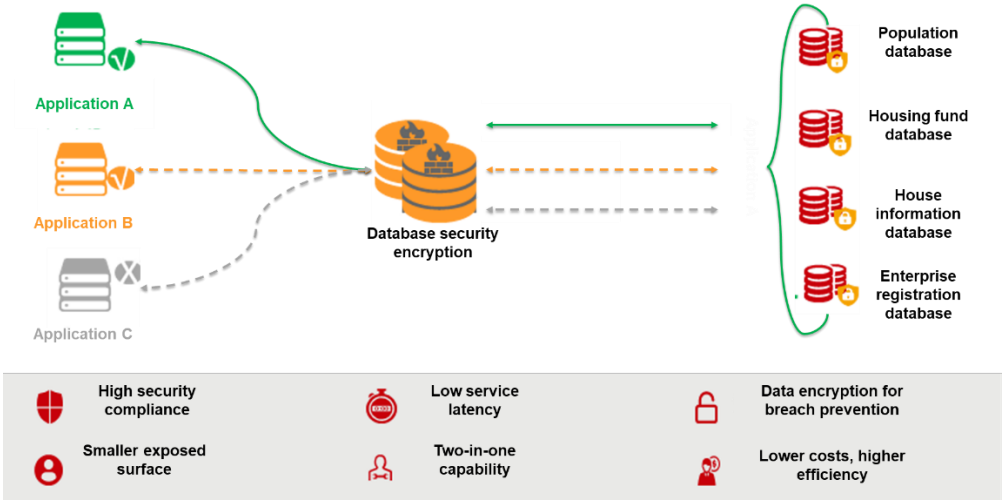
1. Fine-grained behavior audit: Associates access operations at the application layer and database layer and records database access behaviors in detail.
2. Security risk alarm: Monitors ransomware, SQL injection, and risky operations, and immediately generates alarms upon risk detection.
3. Multi-dimensional analysis: Analyzes clues in behaviors, sessions, and statements.
4. Refined reports: Provides reports on session-level behaviors, risk distribution, and compliance.

- **DBSS — Database security encryption**

The database security encryption service supports dynamic storage encryption and multiple encryption algorithms. It can encrypt and decrypt sensitive data, meeting MLPS and cryptography test requirements. In addition, it provides an access authorization mechanism independent of the database to prevent unauthorized access and database cracking by hackers, ensuring database compliance and security.

The data security encryption service prevents data breaches caused by database password leakage, advanced persistent threats (APTs), or improper internal management. The service can be installed using plug-ins, eliminating the need for reconstruction and making it ideal for migrating both new and legacy applications to the cloud without any modifications. The encrypted fuzzy query can be executed properly, and no service adaptation is required. With the ciphertext index acceleration technology, the database security encryption service cuts the random query time of ciphertext columns in data tables with 10 million records from 21.7 seconds to 6 milliseconds.

**Figure 6-7** DBSS capability overview (2)




The database security encryption service provides the following core functions:

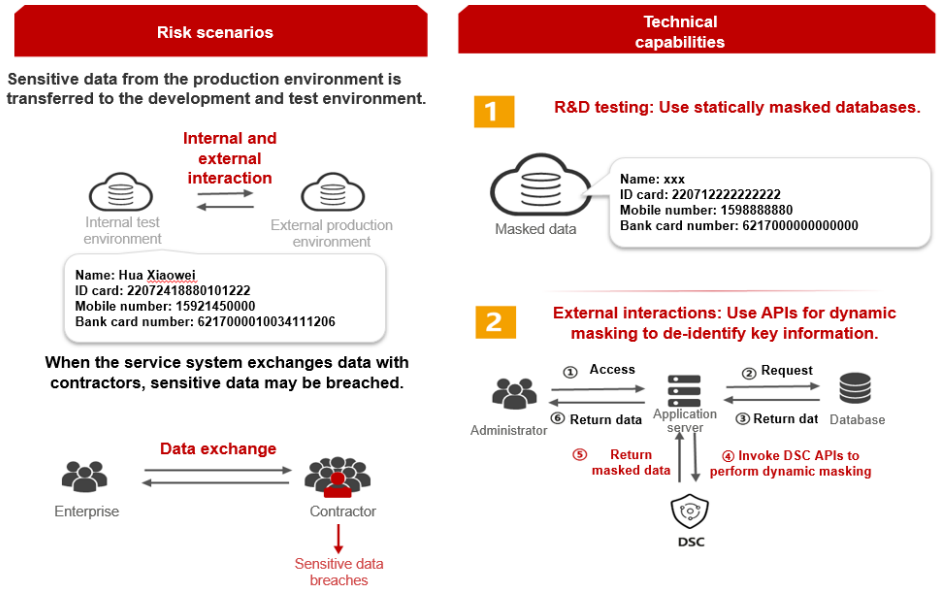
1. Sensitive data identification: Automatically identifies sensitive data based on the signature database and provides a built-in sensitive data signature database.
2. Sensitive data encryption: Supports multiple encryption algorithms, ensuring data confidentiality.
3. Fine-grained access authorization: separation of rights and permissions

4. Operation audit: sensitive operation audit, operation log generation, and event traceability

- **DSC**

  DSC supports static data masking and dynamic data masking. Customers can configure masking rules for specified data to implement static masking of sensitive data, or invoke APIs for dynamic data masking to implement dynamic data masking, preventing sensitive information leakage. During data sharing, customers can use different masking methods to mask sensitive data of different types. Multiple character masking templates have been preset in the sensitive data protection service. For example, sensitive personal data can be masked using character masking, and specific date or number parameters can be rounded up.

**Figure 6-8** DSC data masking



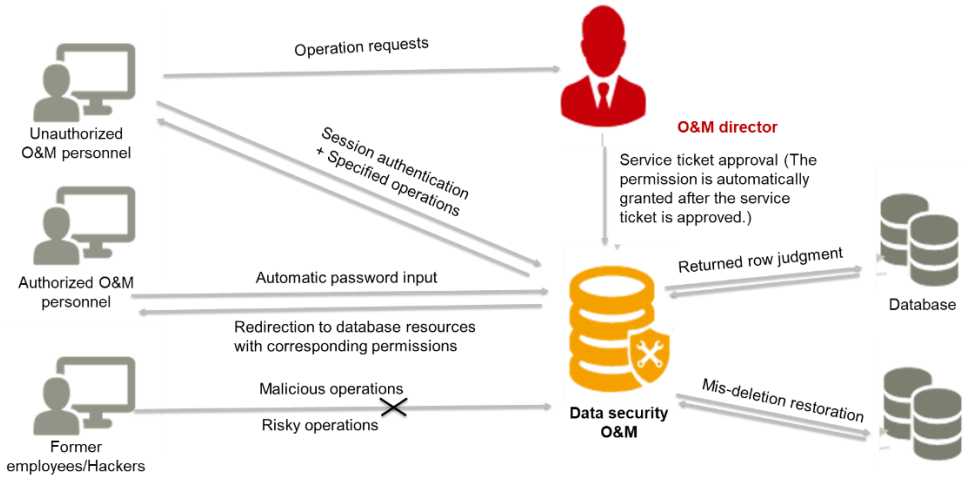

## 6.2.6.3 Cloud Data O&M

- **Database Security Operations and Maintenance (DSOM)**

  DSOM supports independent access control and automatically identifies and blocks high-risk operations. In addition, multiple identity authentication modes are provided for O&M personnel to log in to the database without entering a password, preventing password leakage. Least privilege access, risky operation blocking, and behavior audits are implemented for O&M personnel to ensure production data security and normal O&M operations.

  DSOM supports mainstream databases, big data components, and NoSQL databases. Access control is implemented based on the subject, object, and behavior. Rich database vulnerability information and high-risk operation feature templates are provided to accurately detect risky operations in databases. Protected objects can be flexibly defined and strictly controlled. They cannot be modified, deleted, or viewed without approval. DSOM supports MFA such as SMS verification and FreeOTP, ensuring access security.

**Figure 6-9** DSOM capability overview




DSOM provides the following core functions:

1. **Automatic identification and blocking**: Data security capabilities in the O&M zone, statement-level access control, and automatic identification and blocking of high-risk and other risky operations
2. **Internal threat prevention**: Refined control over data access permissions, multiple identity authentication modes, operation permission approval, and automatic permission revocation
3. **Audit logs and reports:** Comprehensive audit logs, log session playback, and customized reports
4. **Asset management:** Automatic password input, batch changes of passwords, and backup and restoration of tables and data that are mistakenly deleted in the database

### 6.2.6.4 Operation Audit

Cloud Trace Service (CTS) records all operations performed on the cloud in real time. Audit logs are stored and transmitted with strong encryption, and no modification or deletion function or interface is provided, ensuring the integrity of audit logs. Customers can verify and backtrack data through audit and monitoring to ensure that only authorized personnel process data in the cloud environment.

- **CTS**

  CTS records operations on resources in customers' cloud accounts in real time. Each audit log generated for cloud resources records the user, time, and IP address of the operation request, helping organizations analyze unauthorized operations and key resource changes. In addition, real-time SMS and email notifications are supported. Audit logs are stored and transmitted with strong encryption, and no modification or deletion function or interface is provided, ensuring the integrity of audit logs. The permissions to view and access audit logs are assigned and managed by the system administrator in a centralized manner.

- **LTS**

  LTS collects logs from hosts and cloud services. The collected logs can be displayed on the LTS console in an orderly manner and can be stored for a long

time. The collected logs can be quickly queried by keyword or fuzzy query, facilitating efficient tracing of user operations on hosts and cloud services.

- **OBS**

  Customers can use digital watermarks to protect data copyrights, identify data authenticity, and track data transfer. OBS can add text or image watermarks to images. Users can set watermarks for images through the graphical interface on the console, code editing, and interface invoking, and quickly obtain the processed images.

**Service Resources**

- **IAM**
- **CBH**
- **DBSS**
- **DSC**
- **CTS**
- **LTS**
- **OBS**

## 6.2.7 Autonomous Control over Data Destruction

When a customer proactively deletes data stored on the cloud or the data needs to be deleted due to the service expiration, Huawei Cloud will clear the data in compliance with the data destruction standards and the agreement signed with the customer. Before data destruction, customers can use the Cloud Data Migration (CDM) service to migrate content data, implementing independent data control. During data destruction, Huawei Cloud clears the specified data and all copies. For details, see the grace period and retention period rules on the Huawei Cloud official website.

### 6.2.7.1 Customer Data Migration

- **CDM**

CDM allows customers to migrate data among various types of sources, such as databases, data warehouses, and files. It can be used to migrate data within a cloud, between clouds, or between on-premises data centers and clouds.

### 6.2.7.2 Data Destruction

Huawei Cloud provides a controllable data deletion mechanism for customers in the following scenarios:

- Customers can directly delete the data of storage and database services.
- Huawei Cloud recommends that customers encrypt their important data on the cloud. Customers can delete their encrypted data by deleting the encryption keys, preventing data from being recovered to plaintext and leaked before permanently deleted.
- If the subscription of a customer's cloud service resources has expired or the customer's account is in arrears, Huawei Cloud provides a grace period, within which the customer can still access and use the cloud service. If the customer does not renew the subscription or pay off the arrears within the grace period, the cloud service will enter a retention period. During the retention period, the customer cannot access the cloud service but the data stored in the service will

be retained. If the customer does not renew the subscription or top up the account within the retention period, data stored in the cloud service will be deleted. Huawei Cloud provides enough time for customers to determine whether to delete or retain their data.

- If a customer submits a request to deregister their account, all the data of the account will be deleted. In the preceding scenarios, Huawei Cloud will delete all the data and copies from the cloud platform.

### 6.2.7.3 Evidence for Destruction

- **CTS**

  CTS records all operations performed by cloud users, including when and what operations were performed by which users on which resources. When users destroy data, CTS records the operation details so that data owners and data administrators can view, track, confirm, and collect evidence for data destruction operations.

**Service Resources**

- **CDM**
- **CTS**

# 7 Data Neutrality Principle and Transparent Data Processing on the Cloud

Huawei Cloud adheres to the "data neutrality" principle and firmly believes that "Customers own and use their data, and Huawei creates value for customers". Huawei Cloud will never access customer data without authorization. When customers explicitly authorize access, Huawei Cloud will access customers' data in a transparent and visualized manner. Customers can view the data processing operations performed by Huawei Cloud employees on the cloud, and their own data operations are recorded. In this way, data processing on the cloud is transparent and visualized to customers.

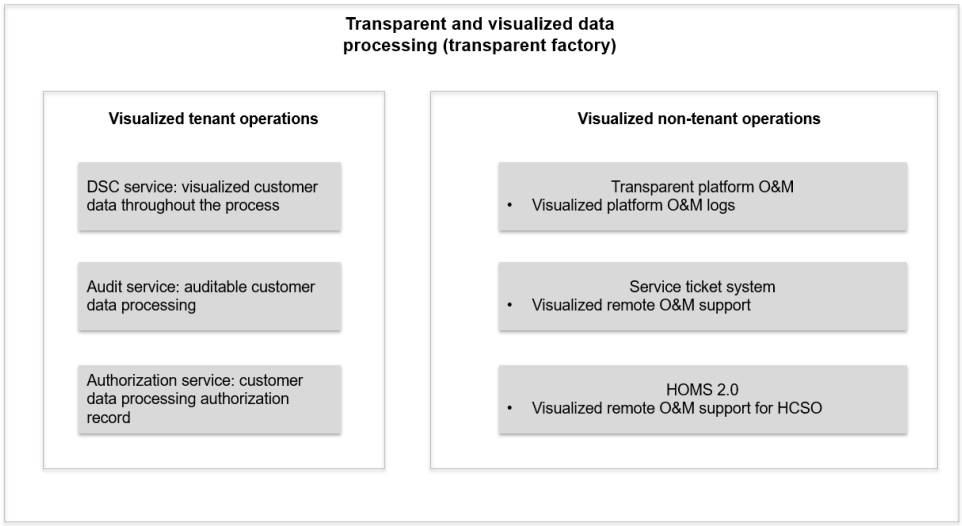
Huawei Cloud plans the transparent and visualized data processing capability to help customers gain a deeper understanding of the processing of content data on the cloud, including Huawei employees' operations authorized by customers, such as service support and O&M, as well as operations performed by customers.

Huawei Cloud always ensures that the content data processing on the cloud is transparent and visualized to customers. Customers have control over their content data on the cloud. In compliance with applicable laws, Huawei Cloud promises not to access customers content data without their authorization.

When a customer requires Huawei Cloud to provide service support, Huawei Cloud ensures that the support personnel can perform related operations only after being authorized by the customer and retains related operation logs for the customer to audit and view.

Huawei Cloud complies with applicable laws and regulations of countries and areas, keeps a close eye on the changes in internal and external regulatory requirements, carries out security standards assessment in related industries, and continuously shares its compliance practices with customers.

**Figure 7-1** Transparent data processing

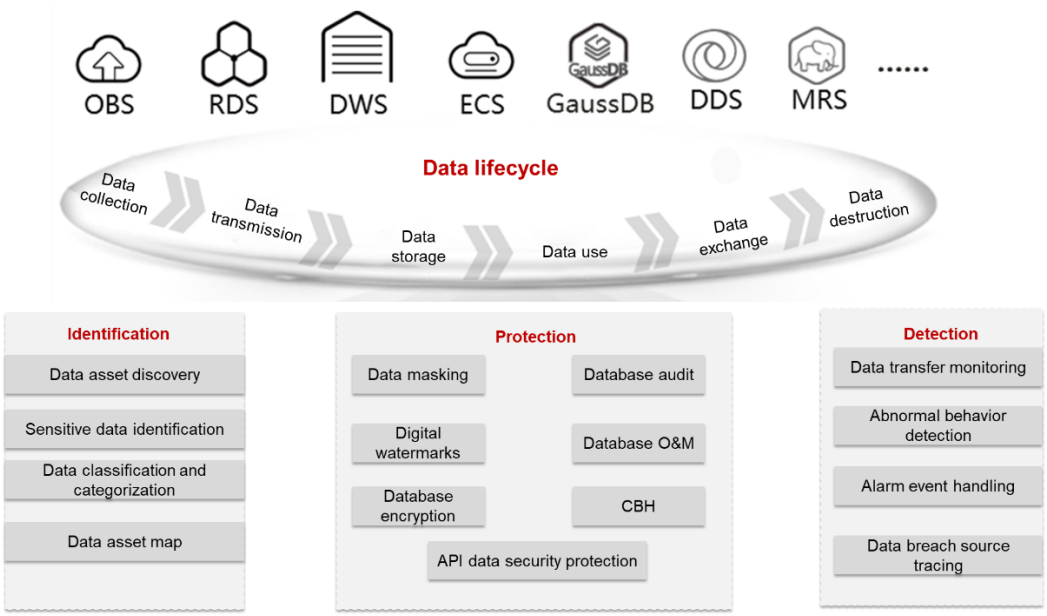



# 7.1 Data Security Operations Platform with Visualized Risks

Centering on data, Huawei Cloud develops full-stack data security services covering the entire data lifecycle. Critical data is protected with in-depth defense mechanisms. Full-stack encryption, customer-held keys, customer-authorized remote O&M, and other measures are adopted to ensure that customers maintain autonomous control over their data security.

**DSC** is a next-generation cloud data security platform that provides basic data security capabilities such as data classification and categorization, risk identification, watermarking and source tracing, and data masking. The asset map gives customers a comprehensive view of their data security on the cloud throughout the data lifecycle. DSC helps customers manage data throughout the data lifecycle.

**Figure 7-2** DSC functions




## 7.1.1 Data Identification

- **Data asset discovery**

  DSC utilizes cloud-native benefits to display distribution, configurations, and external access risks of all data assets on the cloud, including OBS, RDS, CSS, Hive, and HBase. The risk view is mapped with the data classification and categorization result, presenting the risk level for each data category. The Region where each data asset is located is displayed based on the cloud resource VPC, and the risks of data assets are associated with Regions.

- **Sensitive data identification**

  Customers can customize identification dimensions, thresholds, and classification and categorization rules. The regularization and NLP algorithms can efficiently identify sensitive data from massive data within minutes. The distribution and protection status of sensitive data are displayed in detail, providing support for hierarchical data protection policies.

- **Data classification and categorization**

  Data classification and categorization are quickly implemented based on Huawei Cloud classification and categorization templates, industry templates, and customized templates. DSC periodically scans OBS, DB, and Hive to detect sensitive data. It also automatically and quickly identifies sensitive data and personal privacy data based on the expert knowledge base and AI algorithms.

- **Data asset map**

  The risk view is mapped with the data classification and categorization result, presenting the risk level for each data category. The Region where each data asset is located is displayed based on the cloud resource VPC, and the risks of data assets are associated with Regions.

### 7.1.2 Data Protection

- **Data masking**: APIs, 20+ preset masking rules, and customized masking rules
- **Digital watermark**: watermarks for documents, images, and databases; visible and invisible watermarks; and APIs
- **Database audit and O&M:** Allows customers to develop and manage six types of data security protection policies, including database encryption, dynamic masking, O&M, and audits.
- **CBH:** Provides a unified asset O&M entry to make sure that all operations are controllable, manageable, and traceable.
- **API data security protection:** Supports API access control, API risk detection, and API data protection (such as masking and watermarking)
- **Data security operations:** Provides a unified display and management platform for asset statistics, data classification and categorization statistics, threat posture, and response and handling statistics.

### 7.1.3 Data Monitoring

- **Data transfer monitoring:** Monitors data transfer paths and data breach risks in real time, supports collaborative response and handling, and accurately identifies breach sources and paths.
- **Abnormal behavior detection:** Centrally monitors and handles data security events, such as database attacks and API attacks.
- **Alarm management**: Centrally monitors and processes alarms generated by security components.
- **Data breach source tracing**: Centrally extracts database and document watermarks for source tracing.

**Service Resource**

- **DSC**

## 7.2 Transparent and Visualized Storage

Huawei Cloud provides services for customers by Region. A Region is where customers' data is stored. Huawei Cloud will never move customers' data across Regions without their authorization. Before using cloud services, customers are advised to select a Region based on the proximity principle and the laws and regulations of different areas and ensuring that their data is stored in the target location. Customers can select a Region at the initial stage of service purchase. The service deployment location and data retention location can be changed on the Huawei Cloud portal.

## 7.3 Customer Service Response

Huawei Cloud is committed to providing a transparent customer service experience and ensuring that all operations related to customer content data are under customer supervision. By planning the transparent and visualized data processing capability, Huawei Cloud provides services such as CTS and LTS to help customers clearly

understand processing of content data on the cloud, including Huawei employees' operations authorized by customers, such as service support and O&M, as well as operations performed by customers. This transparency not only enhances customers' trust in services, but also provides customers with a user-friendly operation interface, making it easier for customers to manage their data and ensuring that any support behavior is performed with the knowledge and authorization of customers.

Huawei Cloud responds to customers' requests by contractual commitments, response to data subjects' rights requests, and other methods.

1. **Contractual commitment**

   Huawei Cloud has specified its responsibilities and obligations for customers' data protection in related contracts and agreements. Huawei Cloud is responsible for the security of infrastructure and cloud services, and develops and implements appropriate security policies and measures to help customers prevent data breach, damage, and unauthorized access.

2. **Response to data subjects' rights requests**

   Huawei Cloud processes customer requests for data access, correction, deletion, or porting within the legal timeframe and provides clear feedback.

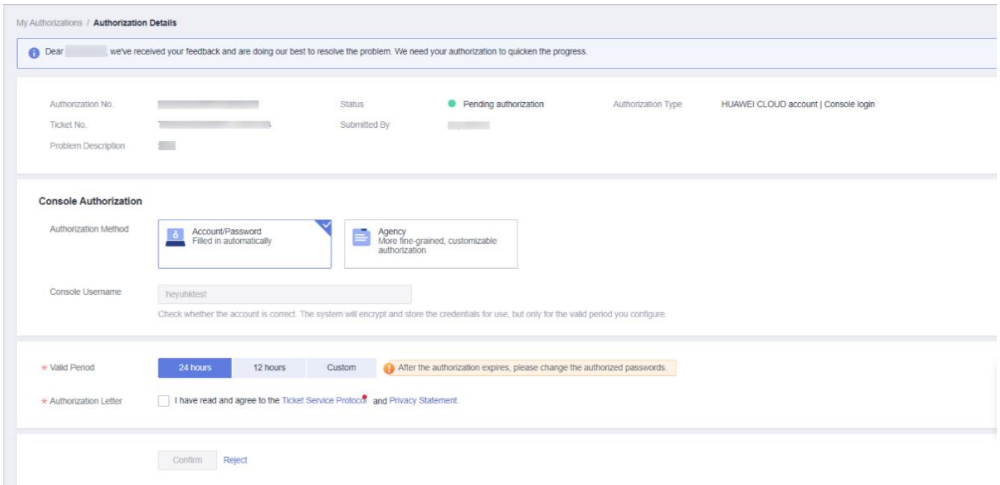
3. **Transparent customer data access by Huawei Cloud authorized personnel**

   In some special scenarios, customers need to apply for support services from Huawei Cloud, and Huawei Cloud may need to access their cloud environments to help them solve problems. To prevent unauthorized personnel from accessing customer data on the cloud and prove to customers that related support personnel access the customer cloud environment only within the authorized scope and time period, Huawei Cloud provides customers with the shared trusted authorization function to ensure that only minimum privileges are granted to Huawei Cloud and Huawei Cloud operations are auditable.

   Shared trusted authorization function:

- Customers can use IAM agencies to specify an authorization method and validity period to ensure that only minimum privileges are granted to Huawei Cloud. If customers enable the CTS service, the entire operation process can be audited by customers.

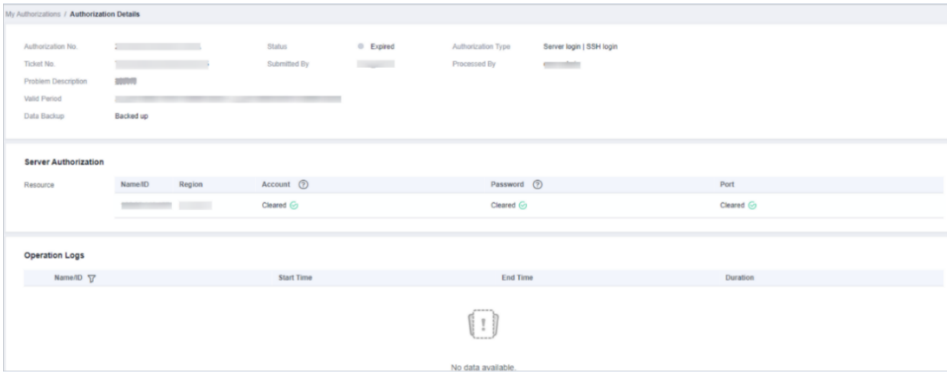
**Figure 7-3** Shared trusted authorization (1)



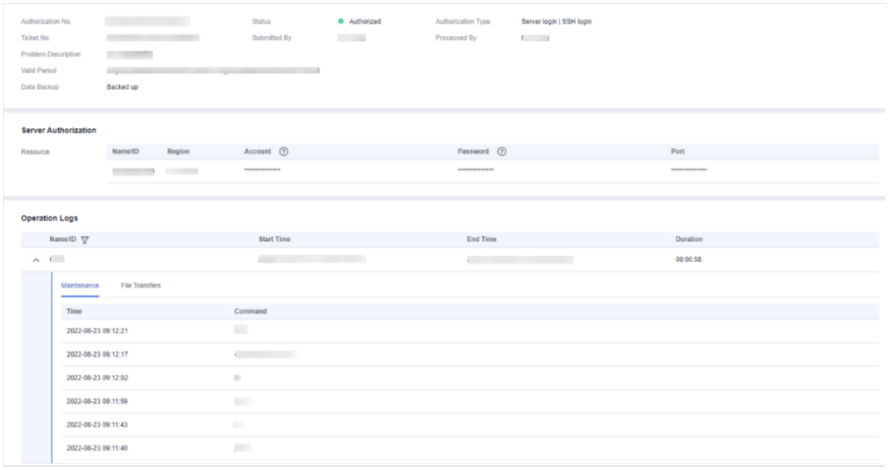
- Customers can use CBH to authorize a specific user to log in to a certain server using SSH. All operation commands and file upload and download records can be viewed on the console.

**Figure 7-4** Shared trusted authorization (2)




- All authorized Huawei Cloud personnel cannot access customers' sensitive personal data. When customers' authorization expires or customers withdraw the authorization, the authorization status is displayed as "Expired", the login account on the console is cleared, and Huawei Cloud cannot access customer data.

**Figure 7-5** Shared trusted authorization (3)




# 7.4 Requirements for Contractors

Huawei Cloud adopts an open and cooperative attitude to build a trust-based cooperation ecosystem that meets the requirements of contractors. Huawei Cloud understands the importance that contractors attach to data security and compliance, and actively shares its compliance practices and technical achievements with them. Through technical exchanges, joint solution development, and joint participation in the formulation of industry standards, Huawei Cloud strives to work with contractors to promote the healthy development of the cloud service market. Huawei Cloud believes that through continuous communication and collaboration, a cooperation

model that meets both regulatory requirements and market requirements can be established to achieve win-win results.

When Huawei Cloud introduces contractors to process data, for example, when Huawei Cloud subcontracts data processing to contractors (involving disclosure to third parties), Huawei Cloud will fulfill its obligation to notify customers of data processors/sub-processors, ensuring that the data access and processing by contractors are also transparent and visualized.

# 7.5 (Outside China) Response to Regulatory Requirements

Huawei Cloud always puts data security first. In compliance with applicable laws and regulations, Huawei Cloud promises not to access customers content data without their authorization. Huawei Cloud is well aware of the importance of complying with local laws and regulations in the increasingly complex global legal environment. As such, Huawei Cloud keeps up with changes in the regulatory environment both within and outside China, and actively evaluates and complies with security standards of related industries, ensuring that Huawei Cloud services meet strict compliance requirements.

1. **Legal and regulatory requirements**

   Huawei Cloud complies with applicable data security laws and regulations of countries and areas where it operates, and actively participates in the formulation of data security standards both within and outside China, ensuring that Huawei Cloud data processing activities comply with laws, regulations, and industry best practices.

2. **Judicial assistance**

   Huawei Cloud does not proactively disclose customer data to law enforcement agencies unless authorized by customers or required by relevant laws and regulations. When Huawei Cloud receives a law enforcement request from a law enforcement agency for customer data, Huawei Cloud will advise the agency to directly obtain data from the customer. If data needs to be obtained from Huawei Cloud for judicial reasons, Huawei Cloud will verify all requests ensuring that they comply with applicable laws, regulations, and judicial procedures. In this case, Huawei Cloud will notify the customer immediately, unless prohibited by law enforcement agencies.

# 7.6 Audit and Certification

With the cyber security and privacy protection certificates, audit reports, and penetration test reports (on the international and European websites) obtained by Huawei Cloud, customers can gain a deep understanding of Huawei Cloud's efforts to protect data security on the cloud and its strong capabilities in ensuring the security of customer data.

Huawei Cloud not only conducts regular self-assessments but also invites third-party organizations to conduct independent audits and shares the results with customers in a transparent manner, helping customers understand how Huawei Cloud protects their data security and privacy.

# 8 Responsibility and Obligation

## 8.1 Customer Data on the Cloud

When customers use Huawei Cloud services, the following two types of data are involved: account data and customer content data.

1. Account data refers to the data provided or generated when customers create Huawei Cloud accounts and use Huawei Cloud services, and it includes but not limited to customers' names, phone numbers, email addresses, bank accounts, and billing details. Huawei Cloud processes customers' personal data in strict accordance with the purposes and scope specified in the *Privacy Statement* and *Huawei Cloud Customer Agreement* on the Huawei Cloud official website. For more information, see the *HUAWEI CLOUD Privacy Protection White Paper*.
2. Content data refers to the service data stored or processed during customers' use of Huawei Cloud services, and it includes but not limited to documents, software, images, and audio and video files. As customers' digital assets on the cloud, content data security is an important concern for all customers to migrate their services to the cloud.

## 8.2 Huawei Cloud Responsibilities

As a cloud service provider (CSP), Huawei Cloud is responsible for providing customers with secure and compliant cloud infrastructure, platforms, and services to ensure that customers can store and process their cloud data in a secure environment. In addition, Huawei Cloud provides customers with a wide variety of data protection technologies and capabilities to help customers better build cloud security capabilities and ensure data security and compliance.

1. Data security protection: Huawei Cloud has developed a comprehensive data security governance mechanism based on five key elements, including organizational responsibilities, policies, processes, tool support, and continuous measurement. In addition, Huawei Cloud has designed and implemented a series of security protection measures at the platform level to protect customer data on the cloud.
2. Data security enablement: Huawei Cloud provides customers with a wide range of services, solutions, and security features to help them enhance data security capabilities and maintain autonomous control over data security on the cloud.

Such services and features include access control and identity authentication, data encryption, sensitive data identification, and database audit.

## 8.3 Customer Responsibilities

Customers are the subject of their data. Customers should formulate data protection policies and take proper measures to ensure data security on the cloud based on their service development requirements and data security risks. They can choose to use the cloud services and solutions provided by Huawei Cloud to store and process data. They can also use appropriate cloud security services or features to harden the security of data on the cloud and comply with applicable laws and regulations. Proper security configurations that should be implemented by customers include OS security configurations, network security settings, data encryption policies, and other security protection policies.

# 9 Security Qualification and Certification

In addition to transforming internal best practices into a range of services to help customers enhance their cloud data security, Huawei Cloud has been actively participating in the development of data security standards both within and outside China. Huawei Cloud continuously contributes to improving industry data security standards and enhancing the overall data security level in the industry.

Huawei Cloud inherits Huawei's comprehensive management system and extensive experience in IT system construction and operations. It actively manages and improves the integration, operations, and maintenance of cloud services. Up to now, Huawei Cloud has obtained many global, regional, and industry-specific security compliance certifications, ensuring the security of customers' business.

For more information about Huawei Cloud security compliance and certificates obtained, select **Trust Center > Compliance** on the Huawei Cloud official website.

Examples of certifications obtained by Huawei Cloud

| Certification | Description |
| --- | --- |
| CCRC data security management certification | The data security management certification of China Cybersecurity Review, Certification, and Market Regulation Big Data Center (CCRC) aims to help organizations strengthen data security practices, comply with national standards, and ensure that organizations meet the basic principles and requirements for network data collection, storage, use, processing, transmission, provision, and disclosure. |
| China Ministry of Public Security MLPS Level-4 | MLPS is the basis used by China's Ministry of Public Security (MPS) to guide organizations in China in building cyber security. It has become a widely followed general security standard across various industries in China. It is divided into levels 1 to 5, with level 5 being the highest and level 4 being the highest level currently attainable by cloud service providers.<br>Huawei Cloud has earned the MLPS level 4 certification, which means that the key Regions, nodes, and system security solutions of Huawei Cloud are designed and built based on the level-4 security protection standards, achieving a multi-layer in-depth protection system. |

| Certification | Description |
| --- | --- |
| China Data Center Alliance (DCA) — TRUCS & Gold O&M | The TRUCS Gold O&M certification is a special assessment of the O&M capabilities of cloud service providers who have already earned the TRUCS certification. This assessment covers 213 areas to review, and an organization must meet standards in at least 180 of them to earn the TRUCS Gold O&M certification.<br>Huawei Cloud has earned the TRUCS Gold O&M certification, a testament to Huawei Cloud's comprehensive O&M management system. It demonstrates that Huawei Cloud has met the certification standards of cloud service operations and maintenance assurance in China. |
| TRUCS User Data Protection Certification | User Data Protection Certification is one of the special assessments of TRUCS. This assessment aims to objectively, comprehensively, and systematically assess the data protection capabilities of cloud products provided by cloud service providers.<br>Huawei Cloud has passed the TRUCS User Data Protection Certification, demonstrating its commitment to security, adherence to business boundaries, and strategic position as a neutral cloud service provider. |
| PCI DSS | The Payment Card Industry Data Security Standard (PCI DSS) is a set of data security standards for payment cards jointly established by five international credit card organizations, including JCB, American Express, Discover, MasterCard, and Visa. It is managed by PCI Security Standards Council. It is globally recognized as the most stringent certification for financial institutions.<br>Huawei Cloud is the first cloud service provider in China to have all its platforms and nodes certified under PCI DSS. This demonstrates that Huawei Cloud can provide customers with financial data security assurance. Customers can deploy financial payment services on Huawei Cloud to ensure compliance with PCI DSS during transmission, storage, and processing of payment card user information. |
| ISO 27001 | ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard focuses on risk management and ensures continuous operation of the organization's information security management system through regular risk assessments and controls. |
| ISO 27017 | ISO 27017 is an international certification for cloud computing information security. Huawei Cloud has earned the ISO 27017 certification, indicating that its information security management capability conforms to the internationally accepted best practice. |

| Certification | Description |
| --- | --- |
| ISO 27018 | ISO 27018 is an international code of conduct that focuses on personal data protection in the cloud. Huawei Cloud has earned the ISO 27018 certification, indicating that it has met the internationally recognized requirements for personal data protection measures on public cloud and can ensure the security of customers' personal data. |
| ISO 22301 | ISO 22301 is a globally recognized standard for business continuity management systems. It helps organizations prevent potential incidents by identifying, analyzing, and warning risks, and develop a comprehensive business continuity plan to quickly recover from interruptions, so that the organizations can ensure the continuity of core functions and minimize potential losses and recovery costs. |
| CSA STAR | The CSA STAR certification was developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI). It aims to address specific issues related to cloud security and help cloud computing service providers show their service maturity.<br>The CSA STAR certification demonstrates that Huawei Cloud has established a scientific and effective management system that can systematically and continuously manage security risks and ensure the confidentiality, integrity, and availability of both its own data and customers' data. |
| ISO 27701 | ISO 27701 specifies the requirements for establishing, implementing, maintaining, and continuously improving privacy management systems. It certifies that Huawei Cloud has a sound personal data protection system. |
| BS 10012 | BS 10012 is a personal data management system standard released by BSI. Huawei Cloud has passed the BS 10012 certification, demonstrating that it has a comprehensive system in place to ensure personal data security. |
| ISO 29151 | ISO 29151 is an international code of practice for personally identifiable information protection. Huawei Cloud has earned the ISO 29151 certification, indicating that it has implemented internationally recognized measures for managing personal data processing throughout data lifecycle. |

# 10 Prospect of Data Security

## 10.1 Continuous Update of Regulations and Standards

The intelligent world is advancing rapidly. Data has evolved from being an outcome of production to a resource, and now it serves as a source for innovation. It significantly influences economic development, social governance, and public life. However, as data is increasingly aggregated, frequently exchanged, and widely accessible, the risks associated with data security and compliance have grown, posing serious threats to national security, social stability, and rights and interests of businesses and individuals.

In response, major economies and areas in the world have established data security regulations and standards to improve data security supervision capabilities and drive data value creation in a secure, compliant, and orderly manner. According to the statistics of the United Nations Conference on Trade and Development (UNCTAD), 77% of countries and areas around the world have enacted legislation on data security and privacy protection. The G20 and BRICS nations have established mutual trust and cooperation mechanisms in data security. International organizations like the United Nations Educational, Scientific and Cultural Organization (UNESCO) and International Telecommunication Union (ITU) are also actively promoting and developing global data security standards.

However, achieving global consensus on data security governance remains challenging due to differences in geopolitics, economies, cultures, and digitalization levels, preventing the realization of the Brussels effect. Although there is widespread recognition of the need for global data security governance and cooperation, data security and cross-border data flows are still subject to individual national laws and regulations, given the strategic position of data in national competition. This constraint hampers the development of the digital economy and digital trade.

Cloud service providers need to comply with applicable laws and standards in different countries and areas, implement industry best practices, and actively contribute to the development and revision of global data security laws, regulations, and standards. They also need to provide users, especially multinational users, with the ability to dominate and control data assets based on local conditions, and work with ecosystem partners to fully meet the security compliance requirements of cloud service users.

# 10.2 Cross-Border Data Flow and Localization Service

As digitalization continues to shape the global economy, data has emerged as a crucial production factor and strategic resource. Cross-border data flows are now integral to not only digital trade, but also digital economy. However, cross-border data flows also cause a series of issues, including national security, data sovereignty, and privacy protection. In response, over 100 countries have enacted data and privacy protection legislation to strengthen the supervision on cross-border data flows. In recent years, there has been a noticeable increase in penalties for violations on cross-border data flows, with fines reaching up to USD1 billion. The complexity and risks associated with complying with cross-border data flow regulations are increasing.

To address these challenges, international organizations like the Organization for Economic Cooperation and Development (OECD) and influential countries such as the United States and European nations are exploring effective mechanisms for managing cross-border data flows. Such mechanisms include Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Digital Economy Partnership Agreement (DEPA), Regional Comprehensive Economic Partnership (RCEP), and EU-U.S. Data Privacy Framework signed in September 2023. In addition, in March 2024, China released the Regulations on Promoting and Regulating Cross-Border Data Flows, which clearly defines legally binding principles and enforcement mechanisms for cross-border data flows.

Cloud service providers need to better understand and adapt to the laws, cultural backgrounds, and rules of different countries while supporting customers' global digital operations, and build a more flexible global cross-border data governance architecture based on the principle of "one country, one policy." This is to adapt to the ever-changing regulatory environment and area differences, provide strong support for business globalization, and offer more choices for customers. In addition, leading cloud service providers should actively promote or participate in the development of global cross-border data flow agreements to reduce obstacles to orderly cross-border data flows.

# 10.3 Technology Innovation and Evolution

Changes in cyber threats, security posture, and attack-defense capabilities promote continuous innovation of cyber security technologies. Technologies such as zero trust, private computation, trusted data space, and post-quantum cryptography drive the data security protection system to a new stage of intelligence.

## 10.3.1 Zero Trust Architecture

In 2010, John Kindervag, an analyst at Forrester Research, first proposed the concept of zero trust. Since then, the value of zero trust has become increasingly prominent. According to Gartner's statistics, by the end of 2024, more than 60% of global organizations have fully or partially implemented the zero trust policy.

Zero trust can extend the static policy protection of limited known locations to the dynamic protection of distributed and large-scale data flows. Zero trust adheres to the principle of "never trust, always verify," effectively restricts attacks such as APTs and ransomware, and effectively controls the "explosion radius" of data breaches and ransomware. It has been proved to be an effective data security protection measure.

Through continuous optimization of internal practices, Huawei Cloud develops zero trust applications for internal use into customer-oriented products and services, and builds a zero trust security system with one security operations center and seven lines of defense. Based on the unified cloud native security architecture of Huawei Cloud, this system consists of SecMaster, an intelligent and simplified security operations center, and seven lines of defense, including physical security, identity authentication, network, application, host, data, and O&M defense, helping enterprises ensure the security of cloud services and data.

## 10.3.2 Trusted Data Space

Since its inception, the data space technology has undergone years of development and industry exploration. It has gradually been understood, accepted, and embraced by government agencies, industry, academia, and research institutions at home and abroad. The data space technology and ecosystem are one of the most suitable solutions for trusted data circulation.

Currently, many major countries have carried out research and practice on trusted data space projects, such as the Giga-smart Access Interoperability for All (Gaia-X) project of the EU and the Health Information Exchange (HIE) project of the United States. In November 2024, China's National Data Administration (NDA) released the *Action Plan for the Development of Trusted Data Matrixes (2024–2028)* to ensure circulation of data elements throughout the entire chain, implement cross-agency data collaboration and convergence, and securely unleash the value of data.

Based on its own practices, Huawei Cloud has explored a set of conceptual framework, design methods, and solutions for data space. It provides users with the Exchange Data Space (EDS) service to help them build data exchange space that is under their own control. By integrating data in and outside the user's company, the service promotes the quantification and distribution of data value, forming a virtuous cycle of data generation, exchange, and consumption, fully unleashing the value of data and achieving "trusted, controllable, and verifiable" data exchange.

## 10.3.3 Data Security and AI

In the new wave of scientific and technological revolution and industrial transformation, artificial intelligence (AI) is serving as a key driving force that is profoundly influencing the future direction of society. At the same time, various new types and means of AI-based attacks are continuously emerging, including deepfakes, black market large language models, malicious AI robots, and automated attacks. The rapid development of AI has also intensified data security risks. Data security is a key safeguard for the healthy development of AI, and the use of AI can enhance the comprehensive capabilities of data security. In the future, more AI systems will require the ability to support the provenance and verification of AI generated content (AIGC). Concurrently, stringent technical requirements must be put in place to ensure the security of AI systems and models, as well as the trustworthiness of AI input and output data, thereby mitigating the risk of AI system misuse and safeguarding the value generated by AI.

To achieve both secure AI and AI security, Huawei Cloud uses AI to empower data security management and technologies at every stage. By integrating various AI technologies with traditional solutions, it builds an intelligent data security system for customers. Huawei Cloud has provided security practices of Pangu models as services and launched its end-to-end large model security solution, which features centralized security operations that cover the security of AI environments, data, content, algorithm models, and AI applications. This solution secures a vast range of

models and applications in various industries, and helps customers build secure, trustworthy, and human-centric large model services.

## 10.3.4 Trusted Computing and Private Computation

Data is diverse and susceptible to modification, replication, and damage. These characteristics give rise to significant security concerns during data circulation. With growing awareness of personal privacy protection and stricter legal supervision, users have higher requirements on data security and privacy protection. Against this backdrop, protecting data security and personal privacy while breaking data silos to release the value of data circulation becomes a major challenge in data application.

Private computation protects data security and privacy under multi-party collaboration through methods such as cryptography, trusted computing, federated learning, and secure hardware, making data available but not visible, computable but not identifiable. In this way, it protects data security throughout data lifecycle and fully unleashes data value. According to Gartner, by 2025, 50% of large organizations will adopt private computation to handle data in untrusted environments or use cases of multi-party data analytics.

In addition, Huawei Cloud has launched cloud services with confidential computing capabilities to the industry when building trusted infrastructure. It uses dedicated hardware and firmware to protect customers' application code and data in use from external access, thereby offering hardware-level security. Huawei Cloud offers confidential computing to isolate customers' code and data from the cloud infrastructure and from customers themselves, helping customers deploy applications and process data in a completely confidential manner. This ensures end-to-end data security and privacy, making data available but invisible.

## 10.3.5 Blockchain

The existing centralized data computing will face great challenges. And blockchain-based edge computing is expected to be effective in addressing these challenges. Featuring immutability and traceability, blockchain can effectively ensure data authenticity and quality, forming a solid foundation for high-quality application in deep learning, AI, and other fields. Blockchain can also implement MPC while protecting data privacy. It is expected to address challenges related to privacy protection and data silos, greatly optimize existing data application, and play a significant role in data circulation and sharing.

Huawei Cloud believes that blockchain is the foundation for trust building and is important for building networks that enable trusted credit and value transfer. Huawei Cloud has been actively exploring blockchain research and application scenarios. Drawing on years of experience in core technologies such as distributed parallel computing, storage, network, security, cryptography, and container, Huawei Cloud has launched its Blockchain Service (BCS). The BCS focuses on building secure and reliable blockchain infrastructure to enable users to efficiently build blockchain networks and industry applications. By doing so, the BCS facilitates the trusted and fast flow of funds, goods, and information, promotes efficient trusted collaboration, and ensures lower collaboration costs and higher efficiency.

## 10.3.6 Post-quantum Cryptography (PQC)

As quantum computing advances rapidly, quantum volume that is used to measure the power of quantum computing is growing exponentially. This can effectively solve computational problems, such as large integer factoring and discrete logarithm

problems, thereby cracking related algorithms such as RSA and Diffie-Hellman. This means that the security of traditional public key cryptographic algorithms based on problems in number theory, as well as of their protocols and systems, is threatened by quantum computing. This poses a significant impact on Internet security.

Following the joint release of PQC candidates and guidelines by the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and National Institute of Standards and Technology (NIST) of the United States, countries worldwide have initiated their migration to PQC. Huawei predicts that by 2030, all ICT systems will be either quantum-safe or capable of migrating to PQC. Quantum computing is developing rapidly. As a result, traditional security algorithms will be vulnerable to quantum computer attacks after 2030. It is therefore urgent to migrate to PQC and quantum key distribution (QKD) that are quantum-proof.

Huawei Cloud will actively explore PQC, and conduct research to evaluate the possibility and feasibility of introducing PQC to enhance product security. It plans to apply PQC to products and services as soon as possible to ensure the long-term security of Huawei Cloud products and cloud foundation.

## 10.4 Systematic Data Security Operations

Data security protection is a long-term complex and difficult task due to data variability and mobility, complex application scenarios, and persistent threats. In recent years, data has become a primary target of cyber attacks, with ransomware attacks evolving into organized mature cybercrimes. Such attacks are highly destructive and profit-driven and have caused significant economic losses and data security risks to countries, societies, enterprises, and individuals. Traditional security operations, due to their long cycles, weak analysis, and inefficient collaboration, struggle to address the data security risks of the digital age.

To address the challenges in data security protection, especially major risks of credential leakage and ransomware, Huawei Cloud, following the principle of "systematic construction and constant operations," builds a data-centric and risk-driven in-depth protection system that integrates the zero-trust security model, based on the unified cloud security capabilities and cloud foundation. The system uses Huawei Cloud SecMaster as the next-generation security operations center and works with the cloud-native DSC to provide integrated data security capabilities, such as data classification and categorization, data anonymization, data watermarking, and API data protection. In addition, it uses an asset map to display the overall data security situation on the cloud, enabling more intelligent, faster, and multi-dimensional detection of and response to data security threats. With this system, enterprises can easily migrate data to the cloud and perform intelligent upgrade on the cloud, achieving "no breakdowns, no data loss, and no regulatory violations."

## 10.5 Data Security Ecosystem Cooperation and Mutual Success

Today, the rapidly evolving global digital economy presents a significant historical opportunity, marking an irreversible shift towards digital and intelligent transformation as well as globalization. Protecting the security of data, a strategic resource, has become increasingly vital. This urgency is heightened by the escalating sophistication of illicit data markets and the growing prevalence of organized cybercrime gangs that

target data security. These escalated attacks cause unprecedented harm and continuously challenge existing data security governance means. This problem has transcended traditional network boundaries as well as national and regional borders and becomes a pervasive global threat.

Faced with complex data security threats, working alone is not enough. Fostering a security ecosystem for win-win cooperation is the right path to take. Huawei Cloud advocates open collaboration across the entire industry and ecosystem to jointly address data security challenges in the digital intelligent era and create a secure digital world together. We will keep open cooperation with industry organizations and ecosystem partners in the government, industry, academia, research, and application fields. Also, we commit to continuously contributing standard proposals, industry understandings, and solutions to industry challenges, with the aim to promote industry development and technological progress. Following the principle of collaborative innovation and win-win convergence, Huawei Cloud provides customers with all-round security protection through a shared responsibility model. By combining the cloud ecosystem and security ecosystem, it seeks comprehensive innovations to make its products and solutions increasingly competitive, and actively works with partners to create an open and cooperative ecosystem for win-win data security protection.