Huawei Cloud Data Security White Paper

Issue 1.0

Date 2022-09-26

HUAWEI

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.huawei.com

Email: support@huawei.com

Contents

1 Overview

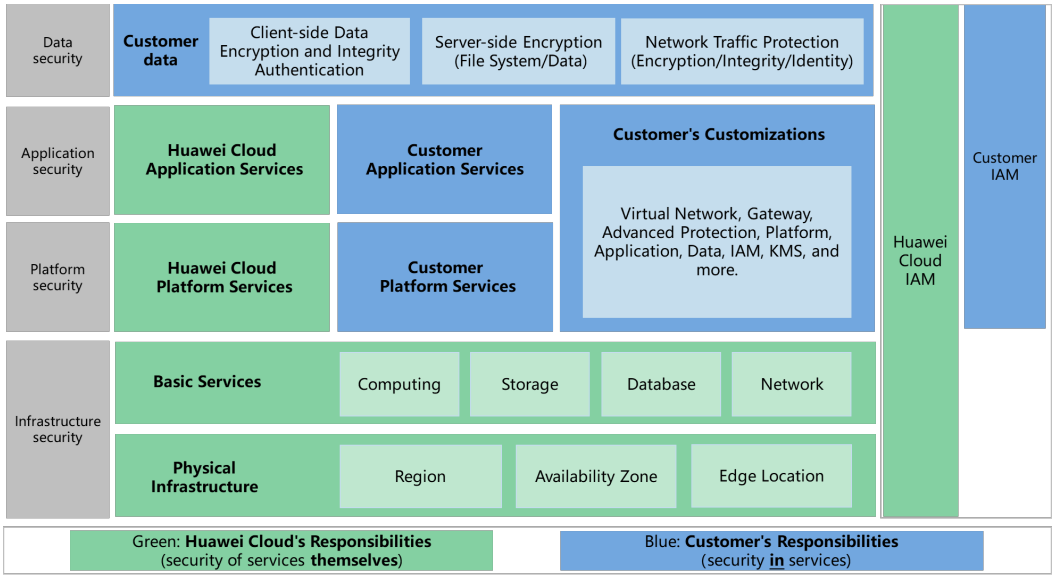
In the digital era, data is a critical resource. Governments, organizations, and individuals place great importance on data sovereignty, data value, and on the rights of data subjects. This means there are significant compliance requirements involved in the face of increasing threats to cybersecurity and privacy. In course of digital transformation, many companies have migrated their data assets to the cloud to take advantage of rapidly developing computing technologies, and cloud security has become a top concern for most of them.

To address this concern and help customers make the most of their data, Huawei Cloud proposed a principle of "data neutrality" – customers own and use their data, and Huawei creates value for customers. The Huawei Cloud data security system is designed to be independent, controllable, transparent, and reliable. Huawei Cloud also promises not to obtain customer service data by technical means, not to force customers to exchange data with Huawei Cloud, and to ensure that data processing strictly complies with all relevant laws and regulations.

2 Huawei Cloud Shared Responsibility Model

The cloud service model is complicated. Data security can no longer be ensured by a single party. Ensuring data security requires Huawei Cloud to work together with customers. To reflect this new reality, Huawei Cloud has defined a shared responsibility model for data security. This model combines common industry practices with specific best practices learned from experience. The model helps clarify the responsibilities of the parties involved and ensures that all data is protected. The following figure illustrates who is responsible for what.

Figure 2.1 Shared responsibility model for Huawei Cloud data security



- **Definition of the customer data in the cloud**

  When customers use Huawei Cloud services, there are two types of data generated: account data and content data.

  Account data refers to the data provided or generated when the customer creates a Huawei Cloud account and uses Huawei Cloud services, including but not limited to their name, phone number, email address, bank account, and billing details. Huawei Cloud processes customer's personal data in accordance with the purposes and scope specified in the *Privacy Statement*

and *HUAWEI CLOUD Customer Agreement* on the Huawei Cloud website. For more information, see the *Huawei Cloud Privacy Protection White Paper*.

Content data refers to the service data stored or processed during use of Huawei Cloud services, including but not limited to documents, software, images, and audio and video files. Content data is customer's digital assets on the cloud. Keeping data assets on the cloud secure is of critical importance to data asset owners. This white paper focuses on how Huawei Cloud protects content data.

- **Huawei Cloud's responsibilities**

  Huawei Cloud is a cloud service provider (CSP) and is responsible for providing secure and compliant cloud infrastructure, platforms, and services to ensure that data can be securely stored and processed on the cloud. Huawei Cloud also provides extensive data protection technologies and capabilities to help customers build powerful cloud security capabilities and comply with data security regulations and laws.

  a. Data security assurance: Huawei Cloud has developed a comprehensive data security governance system that covers five key elements, including organizational responsibilities, policies, processes, tool support, and continuous assessment. Beyond that, Huawei Cloud has designed and implemented a series of security controls at the platform level to protect customer data on Huawei Cloud.

  b. Data security enablement: Huawei Cloud provides customers with a wide range of security services, solutions, and features to help enhance data security capabilities on the cloud and enable complete control over data security. For example, Huawei Cloud Identity and Access Management (IAM), Data Encryption Workshop (DEW), the database audit functions of Database Security Service (DBSS) can help identify sensitive data.

- **Customer's responsibilities**

  The customer is the subject of the data, so customers need to analyze service requirements, evaluate the risk of a data breach, and formulate data protection policies and take appropriate measures to their data on the cloud. Customers can select from range of Huawei Cloud services and solutions for data storage and processing, including cloud security services and features designed to protect data in the cloud and meet regulatory compliance requirements. For example, the customer is responsible for security configurations including OS settings, network settings, data encryption policies, and other security policies.

3 Customer Concerns About Data Migration to the Cloud

After customers migrate their data to the cloud, their data security depends on CSPs' security controls for IT infrastructure. It is understandable that customers may have some concerns about security risks during data transmission, storage, and use. Customers typically demand the following when hosting their data on a cloud:

- They must always know where their data is stored.
- The security of their data in the cloud must be guaranteed.
- There must be no unauthorized access to their data.
- They must be able to freely migrate data from one cloud to another cloud or any on-premises environment.
- Data must be completely, permanently, and irreversibly deleted once such a decision is made.

Targeting these requirements, Huawei Cloud implements the following data security practices:

- **A shared responsibility model** A shared responsibility model is based on the idea that the CSP and the cloud user share the responsibility of protecting data security on the cloud. Either party alone cannot guarantee cloud data security. This shared responsibility model defines the boundaries of the respective responsibilities of the CSP and the customer, so that there are no loopholes.
- **Comprehensive data security governance system**

  Huawei Cloud builds and implements a comprehensive data security governance system that covers organizational responsibilities, policies, processes, tools, and measurement and verification.
- **A secure cloud foundation** Cloud data security depends on a secure and reliable cloud platform. Based on Huawei's over 30 years of security expertise and industry best practices, Huawei Cloud has built secure cloud infrastructure, laying a solid foundation for cloud data security.
- **Flexible choice of cloud security services** Huawei Cloud provides customers with data security services and features covering the entire data lifecycle.

They enable customers to customize their security controls for their data on the cloud to meet diverse needs for different scenarios.

- **Cloud data processing that is transparent to customers**

  Customers can choose the storage location, storage method, and access control for their data. Huawei Cloud will never access customer data without their explicit authorization. When authorized by customers to access their data, Huawei Cloud makes sure that every step of the access is transparent and traceable.

4 Huawei Cloud Data Security Governance System

Huawei Cloud is running a comprehensive, highly reliable, and sustainable data security governance system that covers organizational responsibilities, policy requirements, processes, and technical tools, and provides measurement and verification. This system is built in compliance with related laws and regulations, international industry data security standards, and industry best practices to ensure customer data security.

- **Organizational responsibilities**

  A hierarchical security management responsibility system has been built for cloud data security. The system consists of the decision-making, management, execution, supervision, and support layers.

  - Decision-making: The president of Huawei Cloud is the primary owner for cloud data security and is responsible for decision making related to data security strategies and major security issues.
  - Management: Data security compliance officers and managers are appointed to take charge of routine security management.
  - Execution: The director of each business domain is held accountable for data security risks. They are responsible for identifying risks, setting management objectives, providing countermeasures, and ensuring risk control efficiency.
  - Supervision: An independent inspection team is appointed to promote data security. The team verifies the data security work of each business domain on a yearly basis, tracks identified issues, and helps to resolve them.
  - Support: There are organizations established to support data security operations, including tool development, personnel training, and external communications.

- **Policy requirements**

  Huawei Cloud has established policies, regulations, processes, and operation manuals to specify the purpose, scope, and requirements of data security management. Huawei Cloud requires employees, partners, and external consultants to comply with data security policies and attend security training, to better integrate security policies into the organization.

- **Processes**

  Huawei Cloud has incorporated data security requirements into business processes for continuous security operations. Dedicated data security processes have been added. For example, an application and review process were added for data sharing. Data of different security levels must be reviewed by directors at the corresponding levels, and data security requirements have also been integrated into existing service processes to improve efficiency.

- **Technical tools**

  Huawei Cloud has established data security tools in a platform for customers to manage cloud data securely and efficiently. For example, Huawei Cloud designed and developed the QingTian virtualization platform based on virtualization offloading benefiting from software and hardware synergy. The platform provides a trusted compute environment for cloud data and protects the storage and processing security of customer data on the cloud.

- **Measurement and verification**

  Huawei Cloud has taken a two-pronged approach to the evaluation of data security management. First, a complete measurement system has been established for continuous evaluation. Then second, the data security work is reviewed three times to verify the authenticity and reliability of the compliance.

  Measurement: A wide range of data security metrics are used to assess and monitor data security management for continuous optimization. Three dimensions are measured: processes, results, and operations.

  Verification: A data security specialist from each business domain examines data security operations on a regular basis based on a checklist. The second verification comes from an independent security inspection team that examines the data security work of key services every year. Finally, for the third verification, an independent audit team randomly checks a required number of key services or domains every year and performs data security audits. These three types of verification can make it easier to collect statistics for analysis and can generally improve data security.

5 Safeguarding Platform Security and Cloud Data Security

5.1 Static Data Security

5.1.1 Data Reliability

Data reliability is a key area of focus for Huawei Cloud data security management. To guarantee the stability and reliability of customer data, Huawei Cloud storage services, including Elastic Volume Service (EVS), Relational Database Service (RDS), and Object Storage Service (OBS), all use various technologies to improve data reliability.

In addition to the reliability provided by services, Huawei Cloud Service Level Agreement (SLA) also provides clear service availability commitments for products including EVS, RDS, and OBS. If the service fails to meet the described commitments, Huawei Cloud will compensate the customer in accordance with the SLA.

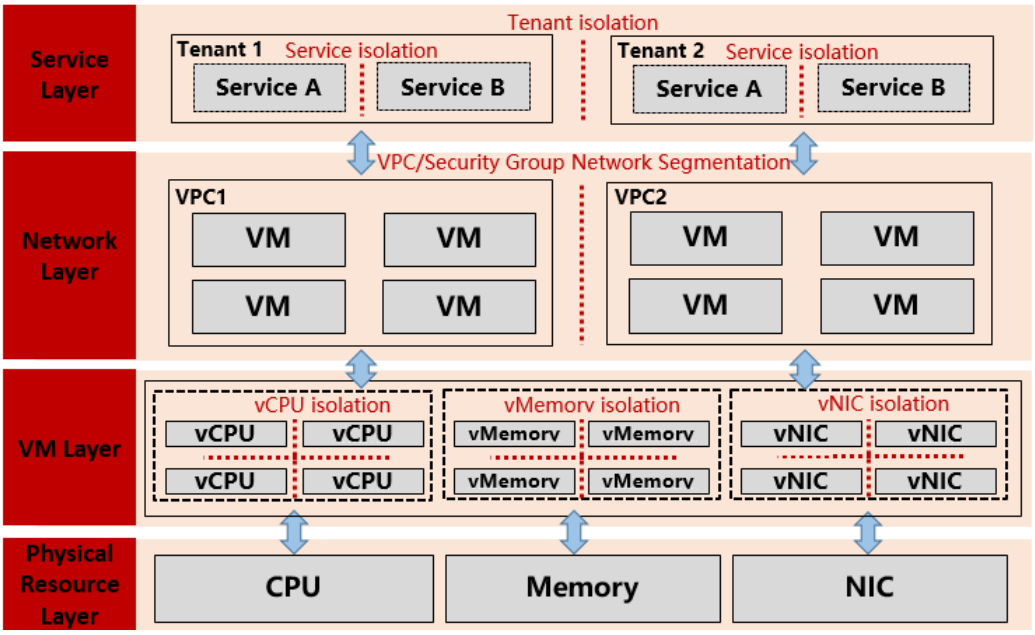
Table 5-1 Huawei Cloud service reliability

Storage Service	Description	Reliability Assurance
EVS	EVS is a virtual block storage service built on a distributed architecture and that supports elastic scalability.	Three-copy redundancy ensures 99.9999999% durability. EVS disks can be backed up and restored using the Cloud Backup and Recovery (CBR) service. Users can also create new disks from backups.
CBR	CBR enables users to easily back up Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), EVS disks, and on-premises VMware virtual environments. If there is a virus attack, accidental deletion, or software/hardware fault, users can restore data to any point in the past when the data was backed up.	Backup data is stored across data centers, delivering 99.999999999% durability.
OBS	OBS is an object-based massive storage service that provides massive, secure, cost-effective data storage.	The data durability is up to 99.9999999999%, and the service availability reaches 99.995%. Data checks: Data consistency is verified using a hash algorithm before and after storage to ensure that the stored data is consistent with what was uploaded. Data slicing: Data can be sliced and stored on different disks. Data consistency is checked in the background, and damaged data can be automatically repaired.
SFS	Scalable File Service (SFS) is a file-based storage service.	The data durability is up to 99.9999999% and the service availability reaches 99.95%. SFS Turbo file systems can be backed up and restored using the CBR service.

Storage Service	Description	Reliability Assurance
RDS	Relational Database Service (RDS) is a cloud-based web service that is reliable, scalable, easy to manage, and ready for use out of the box.	RDS uses a hot standby architecture. If a fault occurs, the system automatically switches over within 1 minute. RDS automatically backs up data daily, with the backups stored in OBS buckets. Backups are retained for up to 732 days. By using the RDS console, users can restore data from backup with just a few clicks.
IMS	Image Management Service (IMS) allows users to easily manage the entire lifecycle of their images. Users can choose from a wide range of public images or create their private images to quickly deploy or batch replicate ECSs.	Private images are stored in multiple copies, with up to 99.999999999% data durability.

5.1.2 Data Isolation

Figure 5-1 Huawei Cloud data isolation solution



Huawei Cloud isolates data on each layer, including the physical resource layer, VM layer, network layer, and service layer, preventing unauthorized access to user data and ensuring data security on the cloud.

- **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.

  - **CPU isolation** refers to the isolation of the VMs from each other and from the virtualization platform itself and to the allocation of VM permissions. CPU isolation is implemented by switching between the root and non-root modes, allocating access permissions differently in each mode, and allocating virtual compute resources in the form of vCPUs. To ensure CPU isolation, the UVP controls the access permissions of VMs for physical devices and virtual running environments. In this way, information and resources for the VMs can be isolated from other VMs and from the virtualization platform. No VM can obtain information or resources from the virtualization platform or from other VMs.
  - **Memory isolation:** The virtualization platform also provides memory resources for VMs and ensures that each VM can only access the memory allocated to it. The virtualization platform achieves this by creating a one-to-one mapping between VMs and physical memory spaces. Address translation is performed at the virtualization layer each time the VM accesses the memory. 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.
  - **I/O isolation:** The virtualization platform provides virtual I/O devices for VMs, including disks, NICs, mouses, and keyboards. Independent devices are provided 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 virtualization platform ensures that only one virtual disk of a VM is associated with any given image file. This ensures that virtual devices used by VMs are mapped to I/O managed objects on the virtualization platform and VMs cannot access I/O devices of other VMs, isolating I/O paths.

- **Network isolation**

  Huawei Cloud isolates cloud data through virtual private clouds (VPCs), which separate networks of different users at Layer 3 and allow users to fully configure and manage their virtual networks. With Virtual Private Network (VPN) or Direct Connect, VPCs can be connected with traditional data centers, allowing for smooth migration of on-premises applications and data to the cloud. Network ACLs and security groups allow for fine-grained configuration of network isolation.

- **Service isolation**

  Huawei Cloud provides isolated, private virtual networks on the cloud based on physical resource isolation and also network isolation technologies like virtual private clouds (VPCs). By default, different VPCs cannot communicate with each other. This helps keep the data of different users isolated, which greatly reduces the risk of a data leak. In addition, you can configure security groups for different types of resources in your VPC. For example, you can isolate OBS resources and RDS instances by associating them with different security groups.

5.1.3 Storage Encryption

Based on industry best practices, Huawei Cloud formulated cryptographic algorithm specifications, including encryption levels and methods, to enhance data storage security. In compliance with these specifications, Huawei Cloud uses the Advanced Encryption Standard (AES) algorithm to encrypt static data stored in cloud infrastructure. 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.

5.1.4 Secure Data Destruction

When customer data is destroyed on Huawei Cloud, the data is deleted, along with all its copies. After a user confirms data deletion, Huawei Cloud first deletes the indexing between the user and the data. Then, Huawei Cloud zeroes out the storage resources involved, such as memory and block storage space. This ensures that deleted data and related information cannot be restored or recovered if those storage resources are later reallocated to other users.

Huawei Cloud also follows comprehensive storage media disposal procedures based on industry standards to ensure data security at the end of the data center media lifecycle. In compliance with the NIST Special Publication 800-88 guideline, data on the storage media that needs to be reused is overwritten by random numbers, or deleted after encryption. Storage media that does not need to be reused is degaussed or physically destroyed.

5.2 Dynamic Data Security

5.2.1 Encrypted Transmission

When data is transmitted between servers and clients of Huawei Cloud and between servers of Huawei Cloud through public channels, the data is protected using the following technologies:

- **Virtual Private Network (VPN)**

VPN establishes a secure encrypted communications tunnel, in compliance with industry standards, between a remote network and VPC. It seamlessly extends services at a local data center to Huawei Cloud, and ensures confidentiality of tenant data in an end-to-end manner. By creating such a VPN tunnel, tenants can conveniently use diverse resources provided by Huawei Cloud, such as ECS and EVS, to migrate services to the cloud and deploy more web servers. By implementing such a hybrid cloud architecture, tenants increase the network compute capability and protect their core data from being leaked.

Currently, Huawei Cloud combines hardware-implemented Internet Key Exchange (IKE) and Internet Protocol Security (IPsec) VPN to provide an encrypted channel for secure data transmission.

- **Application layer TLS and certificate management**

Huawei Cloud provides REST- and Highway-based data transmission. When REST is used, services are released compatible with standard RESTful APIs. Users can use an HTTP client to call service APIs to transmit data. The Highway protocol is a

proprietary high-performance protocol channel that can be used to meet special requirements. In both data transmission modes, transport layer security protocol (TLS) version 1.2 can be used to encrypt transmission, and X.509 certificates can be used for identity authentication and transmission encryption.

Cloud Certificate Manager (CCM) is a one-stop full-lifecycle management service for X.509 certificates jointly provided by Huawei Cloud and various well-known digital certificate authorities. SSL certificates can validate website identities and secure data in transit.

5.2.2 Stable and Reliable Data Transmission

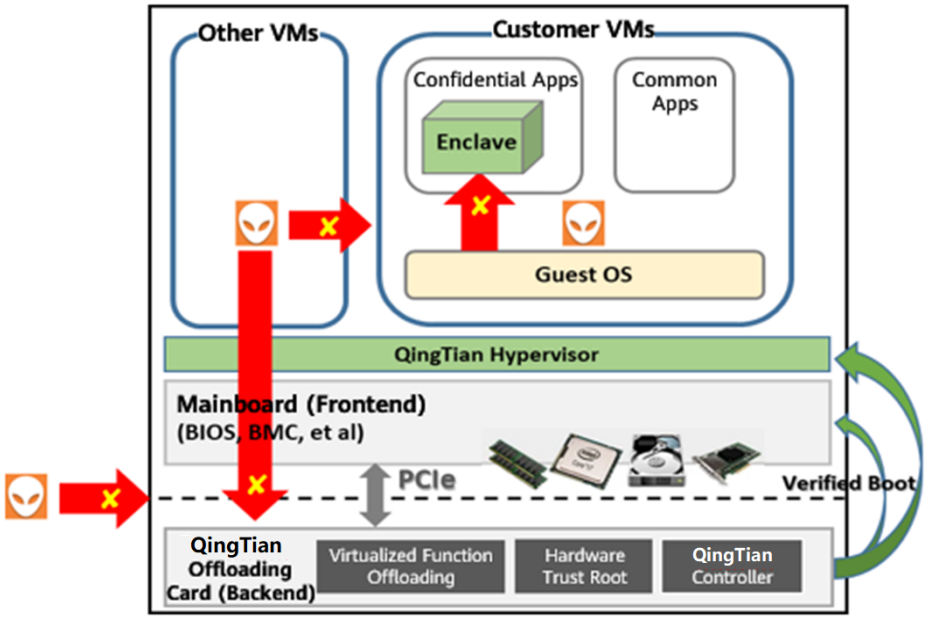
Huawei Cloud provides fast, reliable, secure, and low-latency data transmission. Huawei Cloud offers multi-link DR for customers by allowing them to access their VPCs on the cloud via multiple dedicated connections from different carriers. When one link fails or the entire network of a carrier fails, traffic automatically fails over to another link provided by another carrier, ensuring service continuity.

5.3 Security in Data Processing

5.3.1 Confidential Computing

To ensure customer data is securely processed in the cloud, Huawei Cloud developed the QingTian virtualization (confidential computing) platform. The following figure shows the structure of the security model enabled by QingTian.

Figure 5-2 QingTian security model



The QingTian virtualization platform builds the minimum trusted computing base (TCB) according to design principles such as hardware trust root, enhanced secure boot, firmware anti-tampering, end-to-end encryption, and unidirectional control. It effectively protects customers' cloud data and achieves the following security objectives:

- **Reducing VM escape risks**: The QingTian virtualization platform has a front-end system and back-end system. The latter runs storage virtualization, network virtualization, virtualization management, and security functions, which are functionality modules in a classic virtualization architecture, while the former runs only lightweight hypervisor management programs (such as QingTian Hypervisor) and some of the customer's programs. The simplified hypervisor management program significantly reduces data security risks caused by VM escape.
- **Defending against internal attacks on the cloud platform**: The QingTian virtualization platform supports mandatory encryption of data in transit (such as VPC encryption), persistent data encryption (such as block storage encryption and object storage encryption), and in-memory data encryption (depending on the in-memory encryption feature of CPUs). Secure boot and firmware anti-tampering protect system integrity and prevent internal attackers from tampering with system firmware, executable code, and system data.
- **Reducing data security threats from insiders**: Internal attackers (or rootkits) from the customer can obtain super permissions (such as Linux root permissions) on customers' VMs. Enclave instances can be created to prevent attackers with super permissions from stealing or tampering with important applications and data.

5.3.2 Homomorphic Encryption

Huawei Cloud uses homomorphic encryption (HE) to encrypt data, so that computation can be performed directly on encrypted data without requiring data to the original data. Users can encrypt sensitive data and then send the encrypted data to the cloud for processing and subsequently decrypt the results with a secret key. This improves the usability of data while ensuring data security.

5.3.3 Multi-party Computation

Based on Multi-Party Computation (MPC), Huawei Cloud enables multiple parties from different industries to put their data together and perform joint computation and federated learning and modeling based on the combined data, while ensuring the confidentiality of all data involved. This allows different organizations to share data with each other in a secure manner, maximizing the value of their data.

6 Data Protection Services for Independent Controllable Cloud Data Security

6.1 Data Collection

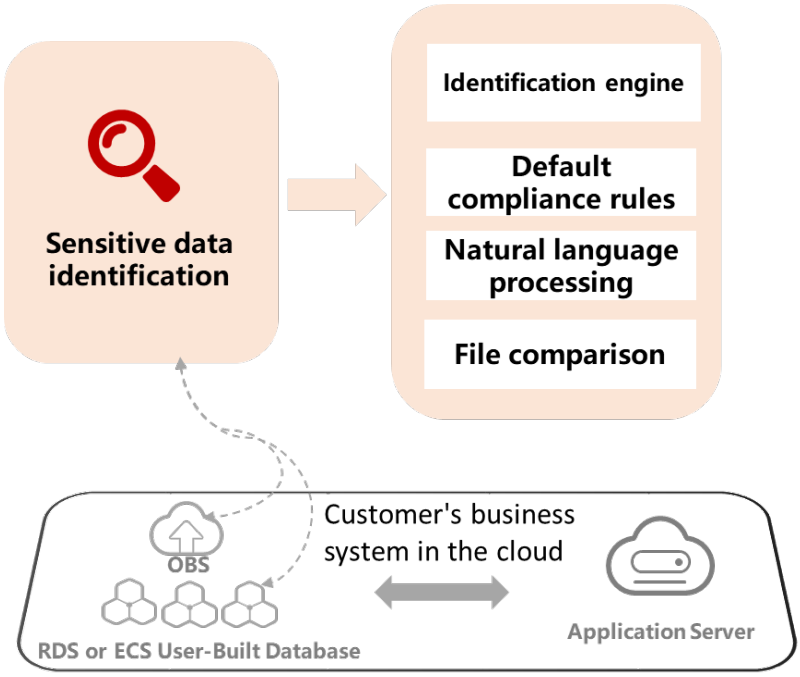
Newly generated, added, updated, and modified data is collected. Huawei Cloud recommends that customers classify and grade sensitive data, analyze risks, and establish measures to protect data security based on risk analysis.

Customers can classify and grade data using Huawei Cloud services. They can define custom data types, identification rules, and sensitive levels to automate identification, classification, and grading of sensitive data.

6.1.1 Data Identification and Classification

- Data Security Center (DSC)

Figure 6-1 Sensitive data identification

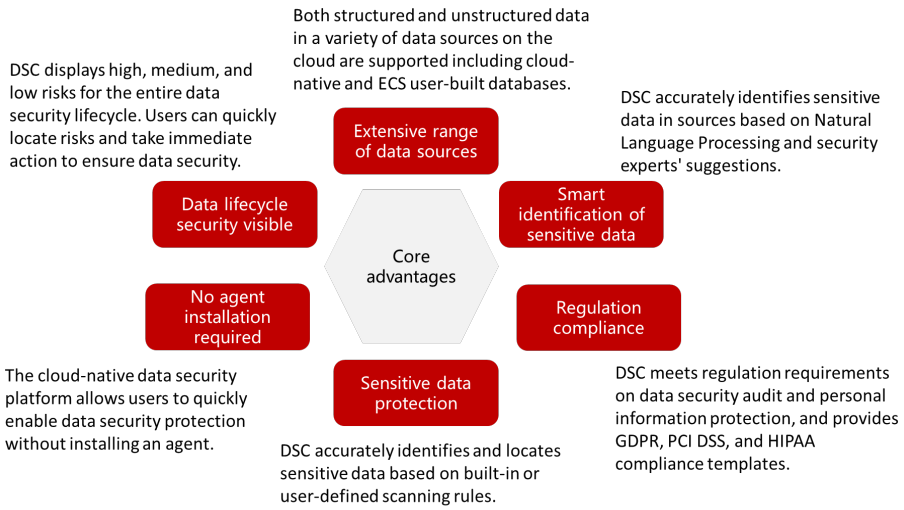


The Huawei Cloud DSC service allows customers to define sensitive data scanning rules, identify sensitive information, and classify data based on sensitive levels. DSC can scan through hundreds of millions of files and terabytes of data to quickly identify sensitive fields or private data. DSC can display overall risks when data is generated thanks to a three-layer data identification engine. DSC supports about 200 data formats, including structured and unstructured data.

According to cybersecurity regulations, a graded data protection system should be established to protect data based on the potential for economic or social impacts, damage to national security, to the public interest, or to the legitimate rights and interests of individuals and organizations if there was data tampering, damage, leakage, or illegal acquisition and use. Important data should be cataloged, and protection of important data must be strengthened. DSC helps customers create rules to identify information in the data catalogs of an industry and comply with related laws and regulations for multi-level data protection.

The following figure shows DSC core advantages.

Figure 6-2 DSC advantages



Services

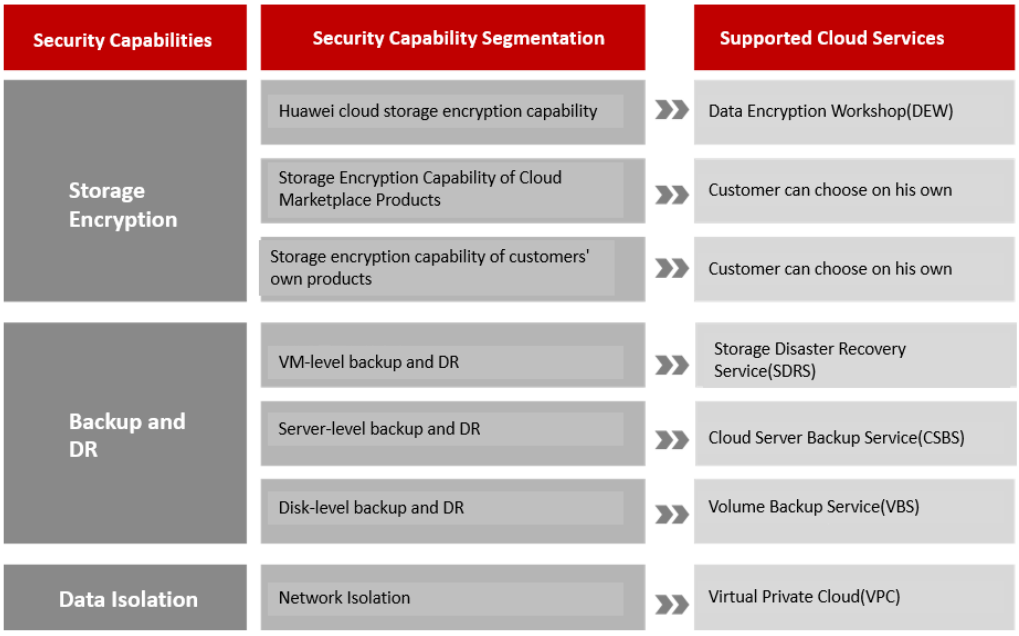
- Data Security Center

6.2 Data Storage

Data storage is any time data is submitted to a certain repository, usually when data is created. In this phase, Huawei Cloud recommends that customers adopt certain protection approaches, such as encryption, backup and disaster recovery (DR), and isolation, for the critical data on the cloud to ensure data storage security.

Customers can use Huawei Cloud services for storage encryption, backup and DR, and to ensure data isolation based on service requirements. For example, when encrypting storage, there are different encryption algorithms with different strengths and key hosting methods. An appropriate algorithm can be selected based on service requirements. There are also various encryption services on the Marketplace, or customers can use their own encryption solutions to control data storage encryption on the cloud. In terms of backup and DR, customers can choose the corresponding backup and DR services for backup and DR protection at the disk, server, and VM layers.

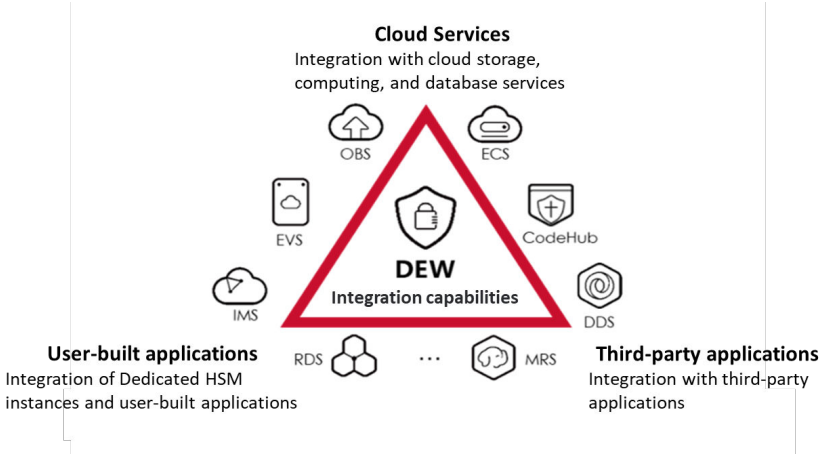
Figure 6-3 Huawei Cloud data storage security capabilities



6.2.1 Storage Encryption

Huawei Cloud packages complex data encryption and decryption logics and key management logics for users to make cryptographic operations simpler and easier. Currently, EVS, OBS, IMS and RDS use a high-performance algorithm to encrypt stored data on the server side. On the Chinese Mainland website, many Huawei Cloud services support cryptographic algorithms issued by Office of State Commercial Cryptography Administration (OSCCA). You can find more details on the Huawei Cloud Chinese Mainland website.

Figure 6-4 Capabilities integrated by DEW



Data Encryption Workshop (DEW)

DEW provides Dedicated Hardware Security Module (HSM), Key Management Service (KMS), and Key Pair Service (KPS), enabling you to easily encrypt and decrypt data. 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.

1. **Dedicated HSM** provides HSMs certified by authoritative organizations and supports key algorithms such as SM1, SM2, SM3, and SM4 (on the Huawei Cloud Mainland website). You can encrypt and decrypt data, sign data, verify signatures, generate keys, and securely store keys. Users can protect the security and integrity of data on ECS and meet regulatory compliance requirements. Users can also manage keys generated by Dedicated HSM, and use diverse algorithms for data encryption and decryption. The following table describes key algorithms supported by Dedicated HSM.

Table 6-1 Algorithms supported by Dedicated HSM

Key Type	Algorithm Type
Symmetric key	AES
	3DES
	DES
	SM1
	SM4
Asymmetric key	RSA_1024
	RSA_2048
	SM2
Digest algorithm	SM3
	SHA1
	SHA256
	SHA384

1. **Key Management Service (KMS)** provides secure, reliable, and easy-to-use key hosting services. KMS uses HSMs to protect Customer Master Keys (CMKs), helping users create and control CMKs with ease. All CMKs are protected by root keys in HSMs to avoid key leakage. The following table describes algorithms supported by KMS.

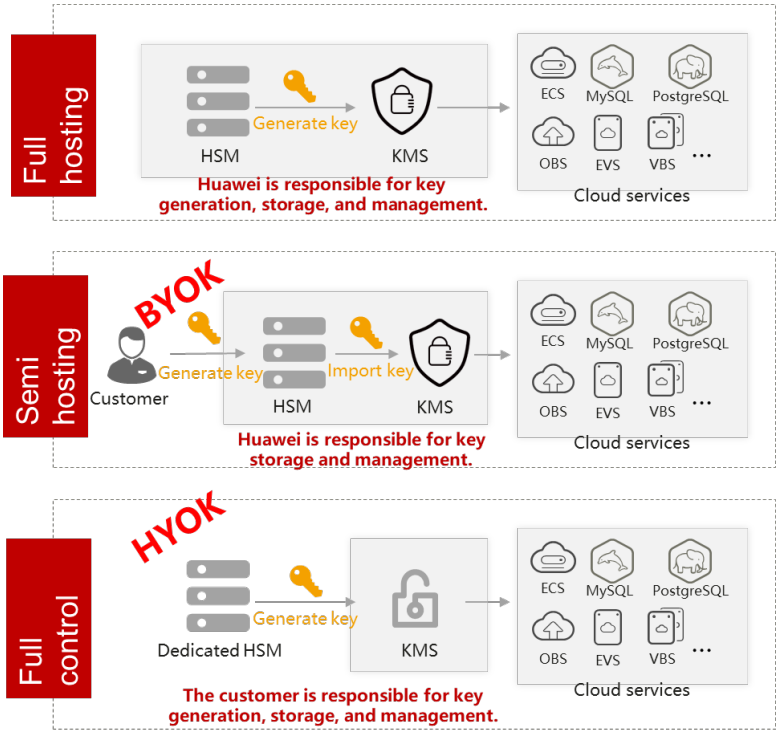
Table 6-2 Algorithm supported by KMS

Key Type	Algorithm Type	Specifications
Symmetric key	AES	AES_256
	SM4	SM4

Asymmetric key	RSA	RSA_2048 RSA_3072 RSA_4096
	ECC	EC_P256 EC_P384
	SM2	SM2

1. **Key Pair Service (KPS)** helps users centrally manage and protect SSH key pairs securely and easily. KPS uses HSMs to generate true random numbers which are then used to produce key pairs. It uses a comprehensive, reliable key pair management solution to help users create, import, and manage key pairs with ease.
2. **Cloud Secret Management Service (CSMS)** provides secure, reliable, and easy-to-use secret hosting services. Users or applications can use CSMS to create, retrieve, update, and delete credentials in a unified manner throughout the credential lifecycle. CSMS can help you eliminate risks stemming from insecure practices such as hardcoding, plaintext configuration, and inadequate permissions control.

Figure 6-5 Key management modes



Users can select any of the three modes based on their regulatory, business, or organizational requirements.

1. **Full hosting**: Keys are generated, stored, and managed on Huawei Cloud to minimize key management workloads.

2. **Semi hosting (Bring Your Own Key, BYOK)**: Users import keys that are generated locally or by third party vendors to Huawei Cloud, where the keys are stored and managed.
3. **Full control (Hold Your Own Key, HYOK)**: Users control the generation, storage, and management of keys by using dedicated HSMs provided by Huawei. This is suitable for customers who need to strictly control keys or store particularly sensitive data on the cloud.

KMS can be used directly or integrated with other Huawei Cloud services, making it easy to create and manage keys. Customers can encrypt data with just a few simple settings.

KMS can manage keys and encrypt data for object storage, cloud disks, cloud images, cloud databases, and scalable file storage. It has been integrated with the following cloud services.

Table 6-3 Cloud services integrated with KMS

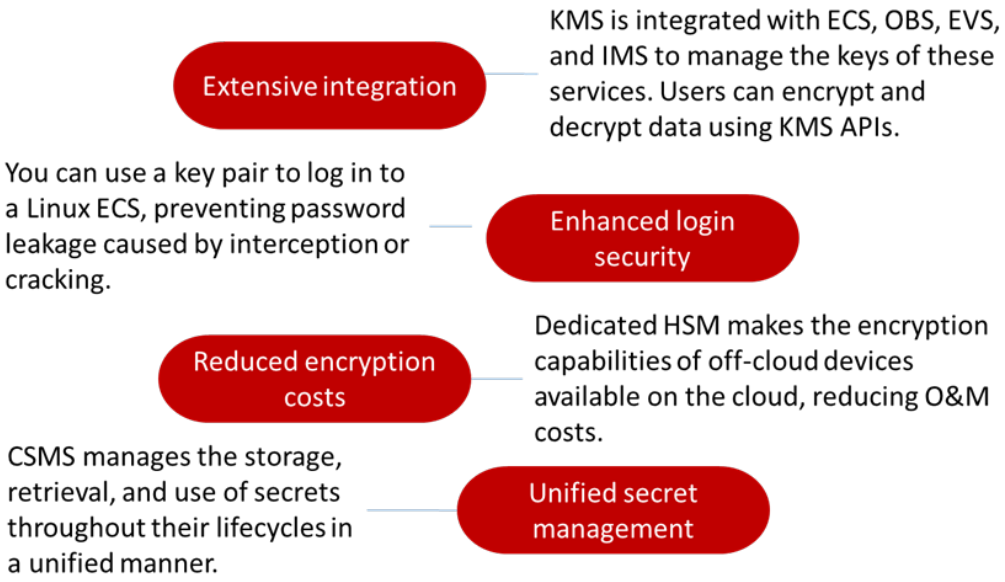
Compute	Elastic Cloud Server (ECS)
	Hyper Elastic Cloud Server (HECS)
	Bare Metal Server (BMS)
	Auto Scaling (AS)
	Image Management Service (IMS)
	Dedicated Host (DeH)
	FPGA-accelerated Cloud Server (FACS)
	GPU-Accelerated Cloud Server (GACS)
	High-performance computing (HPC)
Container	Cloud Container Engine (CCE)
	Cloud Container Instance (CCI)
Storage	Object Storage Service (OBS)
	Elastic Volume Service (EVS)
	Cloud Backup and Recovery (CBR)
	Scalable File Service (SFS)
	Cloud Server Backup Service (CSBS)
	Dedicated Distributed Storage Service (DSS)
	Volume Backup Service (VBS)
CDN & intelligent edge	Content Delivery Network (CDN)
Database	RDS for MySQL

	RDS for PostgreSQL
	RDS for SQL Server
	Document Database Service (DDS)
	GaussDB(for openGauss)
	GaussDB(for MySQL)
AI	Graph Engine Service (GES)
Big data	MapReduce Service (MRS)
	GaussDB(DWS)
	Cloud Search Service (CSS)
	Data Ingestion Service (DIS)
	Data Lake Factory (DLF)
	Data Lake Governance Center (DGC)
	EIHealth
Application middleware	Distributed Cache Service (DCS) for Redis
	Distributed Cache Service (DCS) for Memcached
IoT	IoT Device Access (IoTDA)
R&D and O&M	CodeHub
Video	Video on Demand (VOD)
Security & Compliance	Cloud Certificate Manager (CCM)
	SSL Certificate Manager (SCM)
	Data Security Center (DSC)
	Vulnerability Scan Service (VSS)
Management & Governance	Log Tank Service (LTS)
	Cloud Trace Service (CTS)
Migration	Object Storage Migration Service (OMS)
	Cloud Data Migration (CDM)

For more information about services integrated with KMS, visit the Huawei Cloud website.

The following figure illustrates DEW advantages.

Figure 6-6 DEW advantages



6.2.2 Backup and DR

For enterprises, backup and DR are indispensable to guaranteeing service continuity in emergency scenarios. The DR system should cover the network, application, data and other layers. The data layer focuses on maintaining data consistency and preventing data from being lost, a key link in the DR system. Huawei Cloud provides data backup and DR services at the disk, server, and VM layers.

- Volume Backup Service (VBS)

  VBS allows users to back up server disks while the servers are running. It offers protection from virus attacks, accidental deletions, and software and hardware faults. Backup data is encrypted and stored across multiple data centers.

- Cloud Server Backup Service (CSBS)

  CSBS allows users to create consistency backups for all disks of a cloud server, even when the server is running. It offers protection from virus attacks, accidental deletions, and software and hardware faults. Copies of backup data are stored in different data centers to protect against data center-level faults.

- Storage Disaster Recovery Service (SDRS)

  SDRS provides DR capabilities for ECS, EVS and Dedicated Distributed Storage Service (DSS). By leveraging techniques, such as storage replication, data redundancy, and cache acceleration, it can provide users with cross-AZ, VM-level protection. All it takes is a few simple settings to ensure that if a production site fails, services can be quickly recovered at the DR site to ensure data reliability and service continuity.

6.2.3 Data Isolation

Virtual Private Cloud (VPC)

If a customer wants to use a VM for storage and keep that storage isolated from other resources, they can deploy the VM in a VPC subnet, associate a network ACL with that subnet, and then associate a security group with the VM. Traffic can be controlled at both the subnet and VM levels.

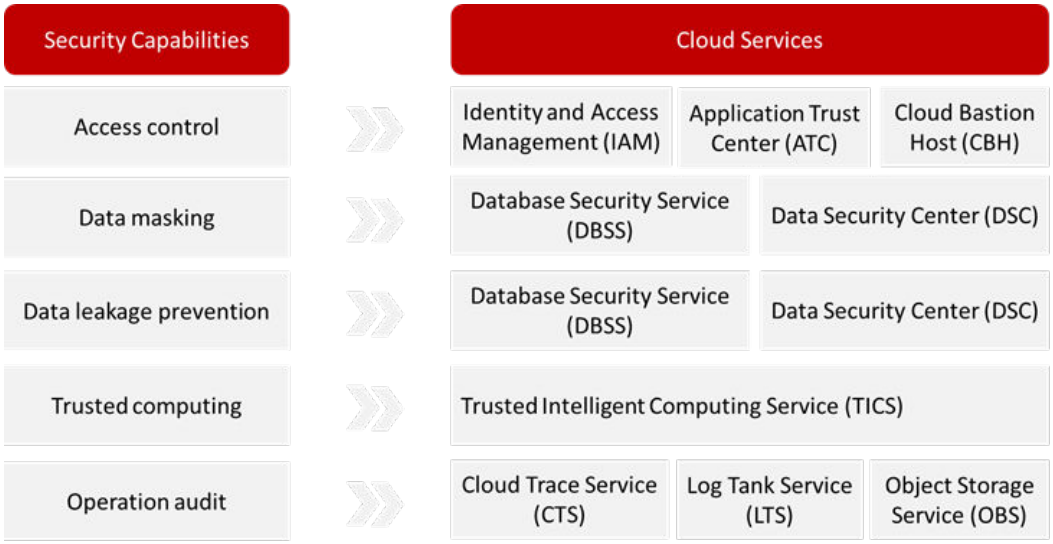
Service resources

- Data Encryption Workshop (DEW)
- Volume Backup Service (VBS)
- Cloud Server Backup Service (CSBS)
- Storage Disaster Recovery Service (SDRS)
- Virtual Private Cloud (VPC)

6.3 Data Usage

Data usage is any time data is viewed, processed, or used in other ways, except for making modifications. In the big data era, people and organizations strive to create more value through data convergence and mining. This creates more risks of information leakage and violations of regulatory compliance. Huawei Cloud services give customers better control over their data security. They provide access control and enable operation audits and data masking. Huawei Cloud services prevent data breaches and support trusted computing. Customers can configure access control policies to prevent unauthorized access to cloud services and applications, or to trace and control various O&M operations. Customers can use static and dynamic masking, data watermarking, risk analytics, and alarm report technologies to prevent data leakage.

Figure 6-7 Huawei Cloud capabilities to secure data usage



6.3.1 Access Control

- Identity and Access Management (IAM)

IAM provides account management, identity authentication, and fine-grained cloud resource access control suitable for the organizational structure of an

enterprise. IAM supports multi-factor authentication (MFA) to secure account logins and important operations. With digital signatures and timestamps, IAM can protect an account from API request tampering and replay attacks. IAM also supports identity federation with enterprises' identity management systems to let enterprise employees log in to Huawei Cloud using single sign-on (SSO).

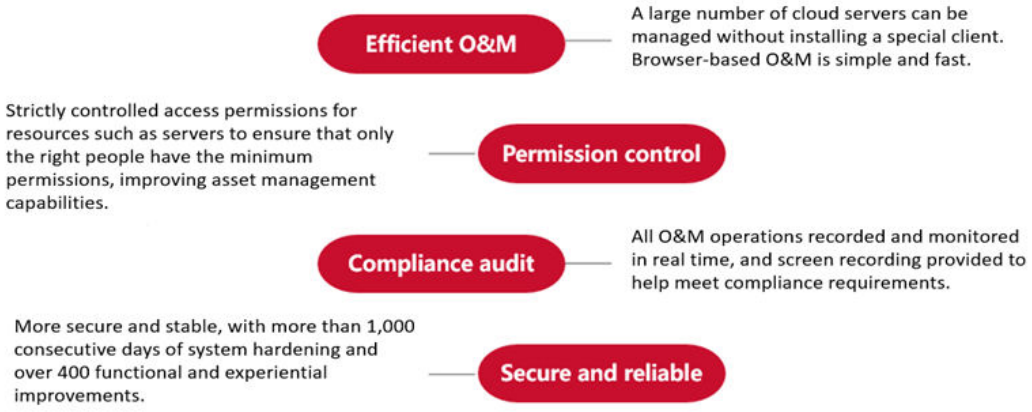
- Application Trust Center (ATC)

  ATC offers a comprehensive overview of security threats to all applications of the customer and enables fine-grained access control built on a zero trust system. ATC can establish behavioral baselines based on user, device, and application access behavior. ATC can quickly detect exceptions and risks together with other security services and dynamically adjust application access control rules.

- Cloud Bastion Host (CBH)

  Malicious operations or misoperations by system O&M personnel may cause greater damage to the system than those performed by ordinary users, as O&M personnel usually have higher permissions and are more likely to access underlying data than others. CBH is recommended to manage and control O&M activities. CBH integrates Huawei's years of experience in security O&M and provides one-stop account management, asset management, access control, and operation audits. It supports multi-factor authentication (MFA) and, cryptographic algorithms issued by OSCCA (for Chinese Mainland website services only) to secure remote login and help with O&M control and compliance audit. Its core advantages are as follows.

Figure 6-8 CBH advantages



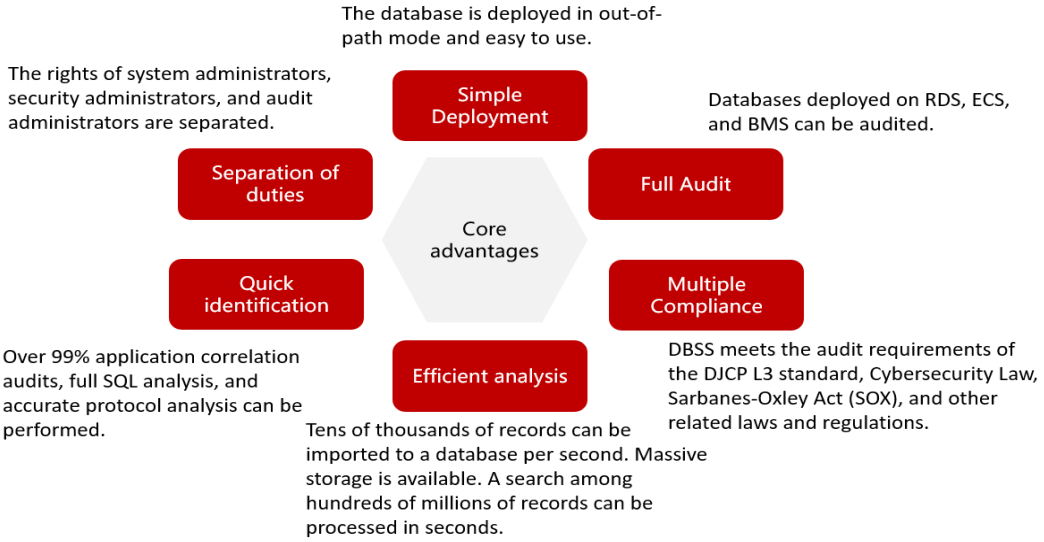
6.3.2 Data Masking and Leakage Prevention

- Database Security Service (DBSS)

Customers can use Huawei Cloud DBSS to protect databases. With patented reverse proxy and machine learning technologies, DBSS provides data masking, database firewalls, and database auditing to enhance data security on the cloud. DBSS can identify sensitive data and hide it from unauthorized users in real time based on configured masking policies. The database performance and data storage are not affected. DBSS can monitor and block attacks like SQL injections in real time, improving database resilience.

The following figure illustrates its core advantages.

Figure 6-9 DBSS advantages

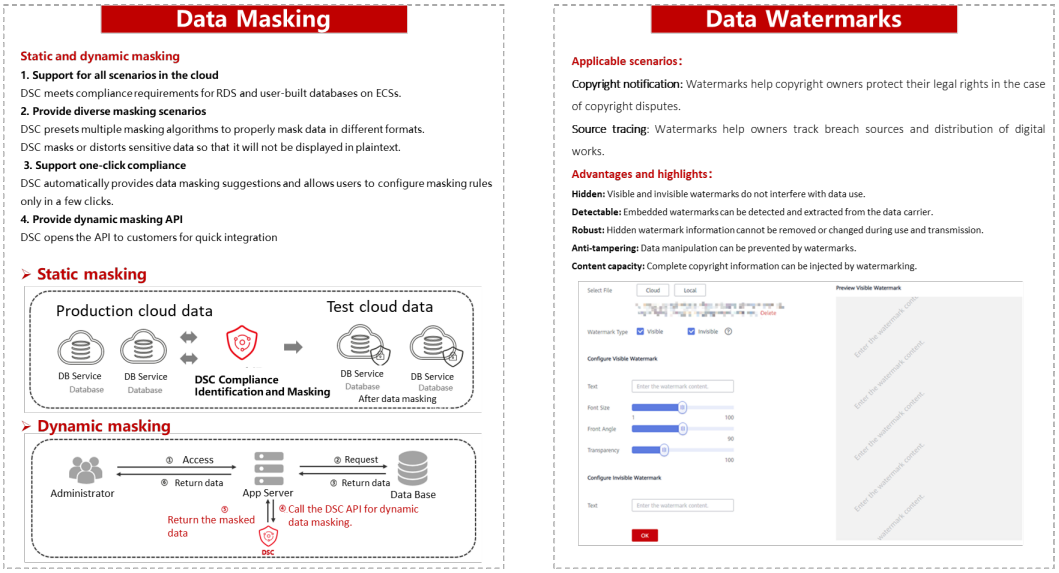


- Data Security Center (DSC)

  Data masking: DSC provides both static and dynamic data masking. Customers can configure masking rules for static masking of specified data assets or call APIs for dynamic data masking. During data use, a range of data masking methods are available for customers to anonymize diverse types of sensitive data. Many character-level data masking templates come preconfigured in DSC. For example, sensitive personal data can be processed using character masking, and dates and numbers can be rounded up using forensic masking.

  Watermarking: DSC provides data watermarks that can be injected into or extracted from documents, images, and JSON strings for source tracing. User information watermarks can be used to protect copyrights and remind users of how the data can be used. If a data breach occurs, watermarks help customers track the source of the breach and find the cause. DSC can identify access key disclosures, generate alarms in a timely manner, and allow users to delete, disable, or whitelist access keys.

Figure 6-10 DSC data masking and watermarking



6.3.3 Trusted Computing

Trusted Intelligent Computing Service (TICS)

Huawei Cloud Trusted Intelligent Computing Service (TICS) breaks down data silos and performs multi-party data analysis and federated learning with data privacy protected. TICS uses technologies such as trusted execution environment (TEE), secure multi-party computing (MPC), federated learning, and blockchain to protect data and audit data transmission and computing. TICS promotes trusted data convergence and collaborations among organizations, deriving extra value from data. The following features are provided for data use security:

- **Trusted compute nodes**: Participants use data source compute nodes to register the sources, establish privacy policies (data masking and encryption), and release metadata, which is independent and controllable. TICS monitors the reliability and helps customers to manage compute node O&M.
- **Federated SQL analysis**: Standard SQL syntax is supported, and a wide range of mainstream data storage systems are connected for converged analysis of multi-party data. Sensitive data can be securely aggregated on compute nodes that run TEE or support MPC.
- **Intuitive supervision**: TICS provides data usage diagrams and blockchain plugins for storage to ensure that data usage is audited and traced.

6.3.4 Auditing

- Cloud Trace Service (CTS)

  CTS records real-time operations on cloud account resources. Each trace logs the user, time, and IP address of an operation, helping organizations analyze unauthorized operations and key resource changes. CTS also supports real-time SMS and email notifications. Traces are stored and transmitted with enhanced encryption. They cannot be modified or deleted, ensuring accurate and comprehensive data. View and access permissions are assigned and managed by the system administrator.

- Log Tank Service (LTS)

  LTS collects logs from hosts and cloud services. The collected logs are displayed on the LTS console and can be stored for long-term archival. They can be quickly searched by keyword or fuzzy match to trace any operation from any source.

- Object Storage Service (OBS)

  To protect copyrighted data or to identify and trace data, customers can use digital watermarks. Huawei Cloud's OBS allows customers to add text or image watermarks to images easily with OBS Console, with a little coding, or with an API call. The processed images can then be quickly made available to customers.

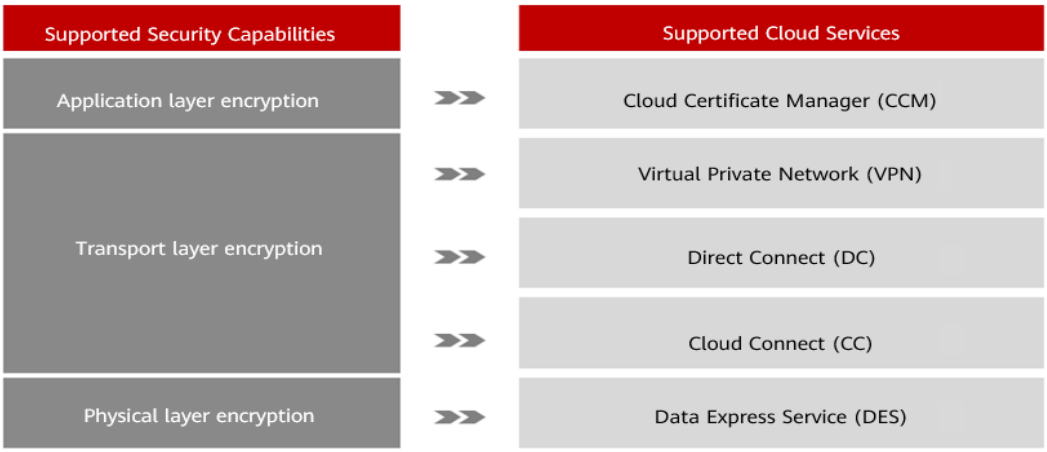
Service resources

- Identity and Access Management (IAM)
- Application Trust Center (ATC)
- Cloud Bastion Host (CBH)
- Database Security Service (DBSS)
- Data Security Center (DSC)
- Trusted Intelligent Computing Service (TICS)
- Cloud Trace Service (CTS)
- Log Tank Service (LTS)
- Object Storage Service (OBS)

6.4 Data Transmission

Data transmission refers to the data that is transmitted from a source to a terminal over a network. To secure data in transit, it should be encrypted.

Figure 6-11 Huawei Cloud data transmission security capabilities



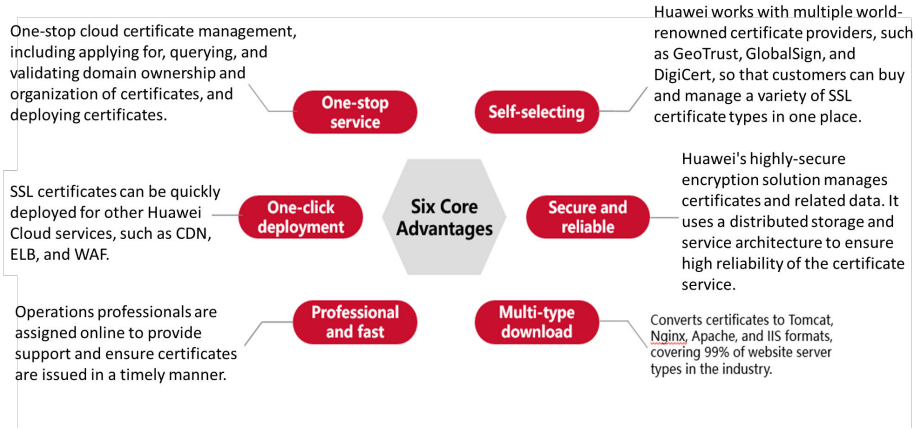
Huawei Cloud provides multiple transmission encryption solutions to meet requirements for different service scenarios. Customers can select whichever one is best suited to the specific service scenarios to secure data in transit.

6.4.1 Transmission Encryption

- Cloud Certificate Manager (CCM)

When services are provided over the Internet, Huawei Cloud CCM makes it easier for users to trust a website. CCM works with world-renowned certificate authorities, such as DigiCert, GlobalSign, and GeoTrust, to provide SSL certificates. Customers can apply for and configure SSL certificates for their websites to authenticate website identity and encrypt data in transit. CCM also provides CFCA certificates, which are available only in the Huawei Cloud Chinese Mainland website. Its core advantages are as follows.

Figure 6-12 CCM advantages



- VPN

Customers whose services are deployed in a global hybrid cloud environment can use Huawei Cloud's VPN, Direct Connect, and Cloud Connect services to enable interconnection and secure data transmission between different regions.

Using Huawei's dedicated devices, VPN creates secure and reliable encrypted transmission channels between local data centers and Huawei Cloud VPCs and between Huawei Cloud VPCs in different regions.

- Direct Connect

Direct Connect uses carriers' private lines to provide dedicated encrypted transmission channels between on-premises data centers and Huawei Cloud VPCs. These lines are physically isolated to ensure security and stability.

- Cloud Connect (CC)

CC is a one-stop cloud connection service built based on Huawei's years of experience in operating IT infrastructure and leveraging their global network layout. It can help customers quickly establish private networks connecting on-premises data centers and VPCs and can also connect VPCs across clouds, greatly facilitating customers' global expansion while also ensuring the security.

- Data Express Service (DES)

DES is a massive data transmission service provided by Huawei Cloud. It provides customers with physical devices, such as Teleports or disk drives, which can then

be used to transmit data to Huawei Cloud. Teleport supports AES-256 encryption, which automatically encrypts data. Users keep the encryption keys themselves. All data is encrypted during transmission to ensure data security in transit.

6.4.2 Cross-Border Data Transfer Management

Customers may need to transfer cloud data across borders for business purposes. When doing so, they need to comply with applicable laws and regulations, such as the EU General Data Protection Regulation (GDPR), China's Personal Information Protection Law, and Data Security Law. The compliance requirements depend on the type of data.

Huawei Cloud helps customers comply with data protection laws and regulations in more than 70 countries. You can go to the Huawei Cloud Trust Center for more information.

Services

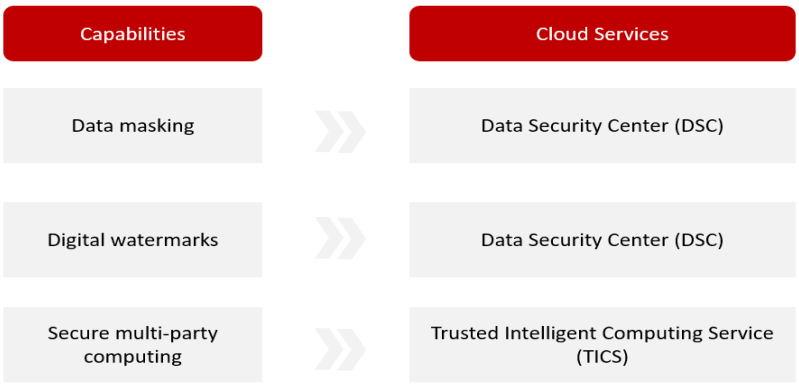
- Cloud Certificate Manager (CCM)
- Virtual Private Network (VPN)
- Direct Connect
- Cloud Connect (CC)
- Data Express Service (DES)

6.5 Data Sharing

Data sharing is any time data exchanges between users, customers, and partners. Data sharing is a prerequisite for data convergence and data mining. It eliminates information silos and derives extra value from data. To ensure data security, customers are advised to strictly control data access and transmission to ensure data sharing secure.

Data masking, watermarking, and secure multi-party computing services are recommended.

Figure 6-13 Huawei Cloud data sharing security capabilities



6.5.1 Data Masking

Data Security Center (DSC)

DSC supports static and dynamic data masking. DSC allows customers to configure masking rules for static masking of specified data assets or to call APIs for dynamic data masking. During data sharing, customers can use different masking methods to anonymize different types of sensitive data. For example, sensitive personal data can be anonymized using character masking, and sensitive enterprise or device data can be masked by keywords.

6.5.2 Digital Watermarks

Data Security Center (DSC)

DSC provides data watermarks that can be injected into or extracted from documents, images, and JSON strings. Watermarks are widely used in government departments, medical institutions, financial institutions, and scientific research agencies. They are generally used for copyright protection and source tracing.

- **Copyright protection**: In scenarios where important documents and images need to be provided to third parties, watermarks can be injected into the files to specify the copyright owner.
- **Source tracing**: When data is shared with an internal third party, user information can be watermarked to remind users of how the data can be used. If a data breach occurs, watermarks help customers track the source of the breach and find the cause.

6.5.3 Secure Multi-Party Computation

Trusted Intelligent Computing Service (TICS)

TICS helps organizations break down data silos and perform multi-party joint data analysis and federated computing within and between industries with data privacy protected. TICS connected to multiple mainstream data storage systems for converged analysis of multi-party data for consumers. Sensitive data can then be securely aggregated on compute nodes. Multi-party analysis uses JOIN operators to protect data privacy, multi-party data is encrypted for computing, and the results returned to users are encrypted too.

Services

- Data Security Center (DSC)
- Trusted Intelligent Computing Service (TICS)

6.6 Data Destruction

Data destruction refers to destroying data physically or digitally. When a customer proactively deletes data stored on the cloud or the data needs to be deleted because a service has expired, Huawei Cloud will delete the data in compliance with data destruction standards and an agreement signed by the customer. Important data cannot be restored after being destroyed. Customers are advised to back up or migrate the data before destroying it.

Huawei Cloud provides data migration services to help customer manage data. During data destruction, Huawei Cloud deletes the specified data and all copies.

Customers can view details about the Grace Period and Retention Period on the Huawei Cloud official website, and can use the search function for other

information as needed. They can also find service-specific descriptions about data destruction in service introductions.

6.6.1 Data Migration

Cloud Data Migration (CDM)

CDM allows customers to migrate data between 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.

6.6.2 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 important data on the cloud. Customers can delete their encrypted data by deleting the encryption keys, preventing data from being converted to plaintext and leaked before being 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 the arrears within the grace period, the cloud service will enter a retention period. During this 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 adequate 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.

6.6.3 Evidence of Destruction

Cloud Trace Service (CTS)

CTS records all operations performed by cloud users to monitor who performed operations, on which resources, at what time. If data is destroyed, CTS records the details of what happened so that data owner and administrator roles can view, track, and confirm the destruction, and collect evidence.

Services

- Cloud Data Migration (CDM)
- Cloud Trace Service (CTS)

7 Data Security Principles and Cloud Data Processing Transparency for Data Owners

7.1 Data Storage Location Transparency

Huawei Cloud has launched cloud services in multiple countries and regions. Its infrastructure spans multiple availability zones (AZs) and regions and offers impressive availability and fault tolerance. Each AZ is physically isolated, so it is protected from failures in other AZs. Customers can plan, deploy, and run application systems across AZs to eliminate single points of failure and ensure services can most likely continue uninterrupted, even in the event of a major disaster. For more details, see **Huawei Cloud Global Infrastructure** on the official website.

Huawei Cloud services are divided by region. A region is the physical location where a customer's data is stored. Huawei Cloud will never transfer data between regions without the customer's explicit approval. Customers are advised to select the regions closer to their clients in accordance with service requirements and applicable laws and regulations, and ensure that their data is stored in these regions.

For regional services, customers can select a region during purchase and change the service deployment location and data retention location on the Huawei Cloud portal, if required.

Customers can select regions and AZs for most Huawei Cloud services. There are the following exceptions:

- Domain Name Service (DNS)
- Identity and Access Management (IAM)
- Content Delivery Network (CDN)
- Host Security Service (HSS)
- Compliance Compass (Compass)

- Log Tank Service (LTS)
- Cloud Trace Service (CTS)
- Huawei Cloud Meeting
- Live
- Video on Demand (VOD)
- Domain Name Service (DNS)

  DNS provides highly available and scalable authoritative DNS services. It translates domain names into IP addresses to redirect end users' access requests to corresponding applications. DNS is a free service and is enabled by default.

  On the Chinese Mainland website, DNS is deployed in Chinese mainland regions, and on the International website, it is deployed in CN-Hong Kong and AP-Singapore regions. Huawei Cloud has performed compliance analysis for DNS in compliance with local laws and regulations on data protection (including personal data) of Chinese mainland, Hong Kong, and Singapore.
- IAM

  IAM is a web service for permissions management, access control, and identity authentication. Customers can use IAM to create and manage users and user groups, provide security credentials, and grant permissions to securely control access to cloud services and resources. IAM is a free service and enabled by default.

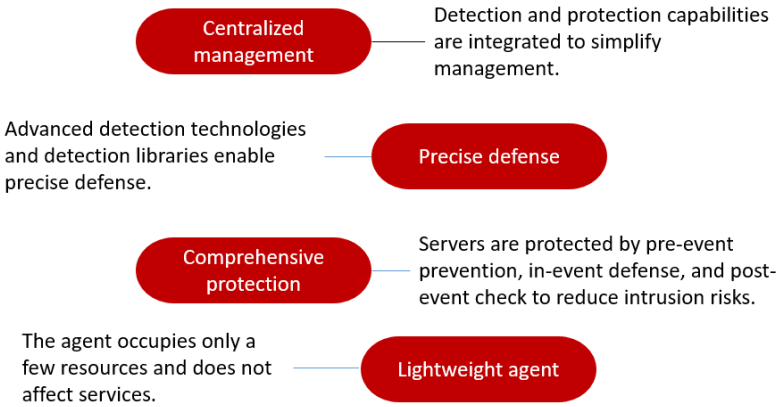
  On the Chinese Mainland website, IAM is deployed in Chinese mainland regions, and on the International website, it is deployed in CN-Hong Kong and AP-Singapore regions. Huawei Cloud has performed compliance analysis for IAM in compliance with local laws and regulations on data protection (including personal data) of Chinese mainland, Hong Kong, and Singapore.
- CDN

  CDN provides fast, stable, and secure global content distribution. It accelerates distribution of multiple services such as websites, images, audio, and video.

  On the Chinese Mainland website, CDN is deployed in Chinese mainland regions. Huawei Cloud has performed compliance analysis for CDN in compliance with local laws and regulations on data protection (including personal data) of Chinese mainland.
- HSS

  HSS is a security manager for servers. It provides asset management, vulnerability management, baseline checks, intrusion detection, application recognition, file integrity checks, secure operations, and web tamper protection functions to help companies detect intrusions in real time and comply with DJCP (MLPS) requirements.

Figure 7-1 HSS advantages



For the Huawei Cloud Chinese Mainland site, HSS is deployed in a Chinese mainland region, and for the International site, it is deployed in the AP-Singapore region. Huawei Cloud has performed compliance analysis for HSS in compliance with local laws and regulations on data protection (including personal data) of Chinese mainland and Singapore.

- Compliance Compass

  Compass is a security compliance assessment and governance platform. Based on Huawei's experience in global security compliance, Compass helps customers to quickly comply with security regulations and industry standards.

  For the Huawei Cloud Chinese Mainland site, Compass is deployed in a Chinese mainland region, and for the International site, it is deployed in the AP-Singapore region. Huawei Cloud has performed compliance analysis for Compass in compliance with local laws and regulations on data protection (including personal data) of Chinese mainland and Singapore.

- LTS

  LTS provides one-stop log collection, log search in seconds, massive log storage, log structuring and transfer. Graphical application O&M, visual analysis of network logs, graded protection compliance, and operation analysis make organization tracking easier.

  LTS is deployed both in the Chinese mainland and in Singapore for use in China and international markets respectively. Huawei Cloud has analyzed and confirmed that LTS complies with local laws and regulations (including protecting personal data) of the Chinese mainland and Singapore.

- CTS

  CTS traces cloud resources for each account. By analyzing operation traces, customers can monitor security, change resources, audit compliance, and locate faults. Real-time trace transfer to OBS can be configured for long-term storage.

  CTS is deployed both in the Chinese mainland and in Singapore for use in China and international markets respectively. Huawei Cloud has analyzed and confirmed that CTS complies with local laws and regulations (including protecting personal data) of the Chinese mainland and Singapore.

- Huawei Cloud Meeting

Huawei Cloud Meeting offers secure and reliable videoconferencing with crystal-clear audio and ultra-HD video. Users join a meeting from a computer, mobile, or fixed room terminal anytime, anywhere.

On the Chinese Mainland website, Huawei Cloud Meeting is deployed in Chinese mainland regions, and on the International website, it is deployed in CN-Hong Kong. Huawei Cloud has performed compliance analysis for Huawei Cloud Meeting in compliance with local laws and regulations on data protection (including personal data) of Chinese mainland and Hong Kong, China.

- Live

  Huawei Cloud Live is the cumulation of years of video expertise. It offers a secure and high-concurrency E2E livestreaming solution while delivering a low-latency HD experience.

  Huawei Cloud has performed compliance analysis for Live in compliance with laws and regulations of regions where Live is being offered.

- Video on Demand (VOD)

  Huawei Cloud VOD is a one-stop service, covering video uploads, automatic transcoding, media asset management, and distribution acceleration.

  VOD is available only on the Chinese Mainland website and is deployed in Chinese mainland regions. Huawei Cloud has performed compliance analysis for VOD in compliance with local laws and regulations on data protection (including personal data) of Chinese mainland.

  If there is any discrepancy between the above service description and the one on the official website, the description on the official website prevails.

- Data storage and management

  The global economy is growing fast, and cross-border data flow has become an important support for economic development. More and more data management regulations and laws are being issued in many countries and regions to meet national or regional data security requirements at different levels. Huawei Cloud services are available in more than 65 countries, and Huawei Cloud has read and analyzed the applicable laws and regulations related to data management in these countries. For details, go to "Trust Center" on the Huawei Cloud International website.

  The compliance content in Trust Center is not and should not be deemed legal advice. The content is for reference only. Customers should consult with their internal legal affairs department before migrating workloads to Huawei Cloud to ensure that their data retention policy is compliant with applicable laws and regulations.

7.2 Data Access Transparency and Visibility

7.2.1 Huawei Cloud Protects Customer Data from Unauthorized Access

Customers have complete control over their content data on Huawei Cloud. Huawei Cloud leverages a comprehensive data security governance system to provide customers with a wide range of security services and features to protect customer data from unauthorized access throughout the entire data lifecycle.

First, the customer maintains complete control over their credentials and permissions for content data. They can take advantage any number of different technologies to protect sensitive data such as security credentials. For example, Huawei Cloud Data Encryption Workshop (DEW) can be used to ensure that only authorized personnel can access a given set of data.

Second, Huawei Cloud's Cloud Trace Service (CTS) can record all operations performed in a customer's cloud environment. CTS lets customers verify and backtrack operations through audits and monitoring to ensure that only authorized personnel can process data on the cloud.

Beyond that, Huawei Cloud implements strict access control on operations on the cloud platform. Huawei Cloud implements strict segregation of duties for employees. Only authorized personnel can access a production environment and only during the specific period they have been authorized for. Major changes to a production environment cannot be implemented unless they have been reviewed and approved.

Huawei Cloud uses role-based access control for O&M personnel, always assigning only the minimum permissions necessary, to ensure that O&M personnel cannot access customer data without express authorization.

Huawei Cloud also implements centralized access, authentication, authorization, and audit for O&M operations. O&M personnel access the O&M environment using two-factor authentication, and then log in to servers via CBH. Credentials for logging in to the target servers are withdrawn by CBH once the O&M tasks are complete and then periodically updated by CBH. In this manner, Huawei Cloud prevents O&M personnel from obtaining credentials for any reason other than O&M purposes.

Huawei Cloud has established a centralized and comprehensive log audit system. All O&M operations performed by internal personnel are recorded by the system. Huawei Cloud regularly monitors and audits activities in the O&M process, and generates alarms for and terminates abnormal operations in a timely manner. Any violations of O&M procedures will be punished in accordance with relevant company regulations.

Furthermore, Huawei Cloud periodically invites independent third parties to assess Huawei Cloud's security compliance with industry standards, such as SOC, C5, and PCI-DSS certification, to validate Huawei Cloud security controls, including how Huawei Cloud effectively protects customer content data from unauthorized access. For example, the SOC CC6.3 addresses that "The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives." Huawei Cloud implements technical and procedural security controls to comply with this standard.

For more information about security compliance certification, go to Huawei Cloud Trust Center.

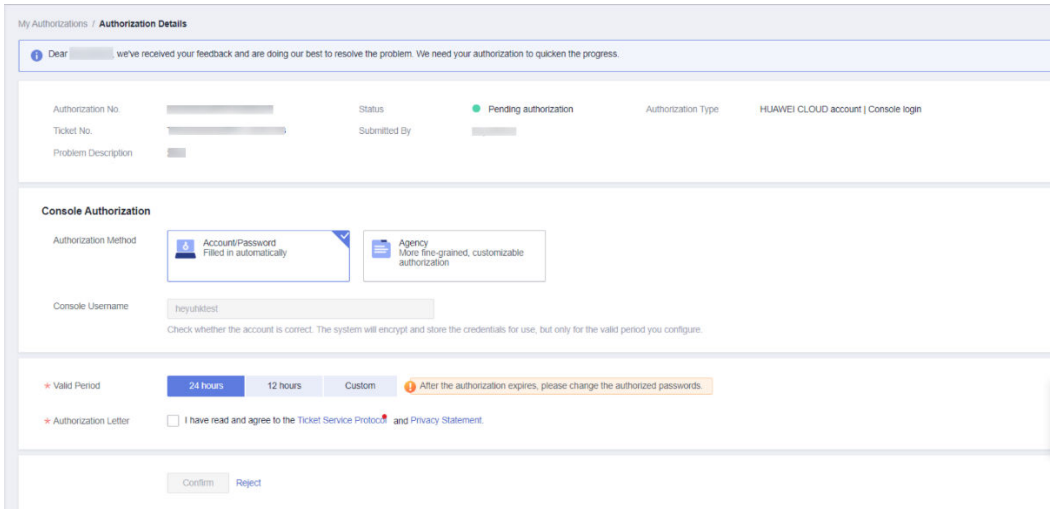
7.2.2 Huawei Cloud Ensures Authorized Data Access Is Fully Transparent and Visible

In some special scenarios, customers need support from Huawei Cloud, and Huawei Cloud needs to access their cloud environment to help solve problems. To

prevent unauthorized access to personal data on the cloud and demonstrate that the cloud environment is accessed only within the scope and for period specifically authorized, Huawei Cloud uses a shared trusted authorization model. With shared trusted authorization, only minimum privileges are granted to Huawei Cloud, and Huawei Cloud's operations are auditable.

The shared trusted authorization has the following functions.

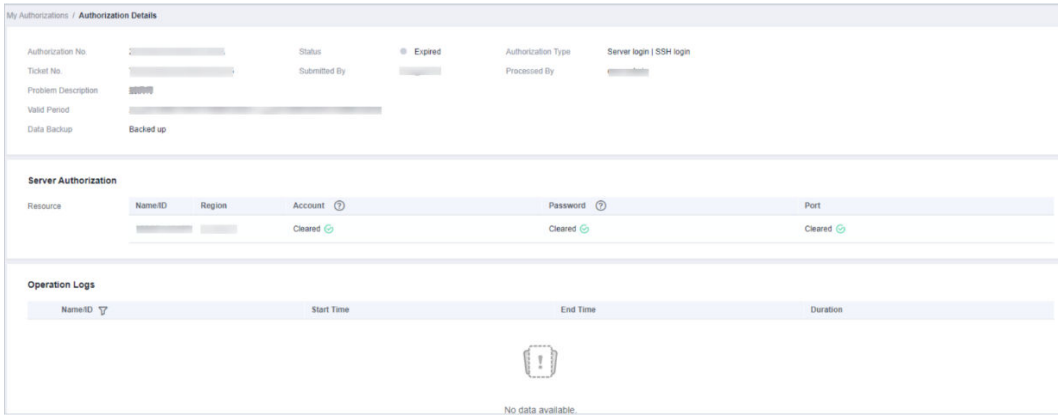
Figure 7-2 Shared trusted authorization (1)



Customers can use IAM agencies to specify an authorization method and validity period to ensure the principle of least privilege is followed. They can also enable Cloud Trace Service (CTS) to audit the entire process.

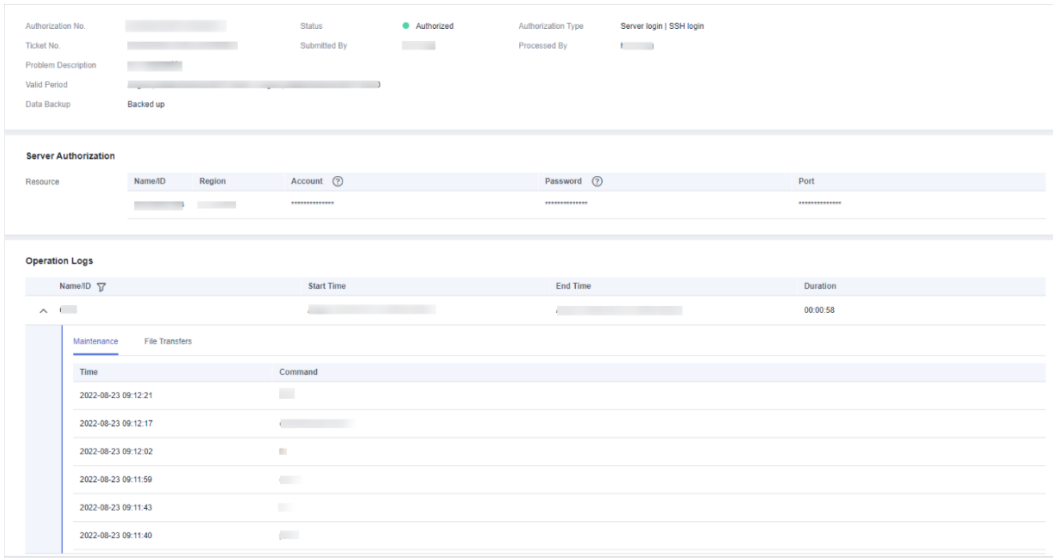
Customers can use Cloud Bastion Host (CBH) to authorize a specific user to log in to a certain server using SSH. All operation commands and file upload and download logs can be viewed on the console.

Figure 7-3 Shared trusted authorization (2)



When an authorization expires, the account status changes to **Expired**. When an authorization is cancelled, the account is deleted from the console. In either case, Huawei Cloud personnel cannot access the customer data anymore. Sensitive personal data is inaccessible for any personnel from Huawei Cloud even if they are authorized to access the customer's cloud environment.

Figure 7-4 Shared trusted authorization (3)



8 Huawei Cloud's Contributions to Data Security and Achievements

Huawei Cloud security products are designed based on Huawei's decades of experience designing security products for their own use as well as extensive industry best practices. Huawei Cloud has helped formulate data security standards in and outside China and is continuously contributing to improving data security standards and improving data security throughout the industry.

Huawei Cloud has been evaluated and has earned certifications from hundreds of security certification bodies from all over the world. Although these certifications cannot speak to Huawei Cloud's entire cloud security capabilities, they are a reflection of Huawei Cloud's achievements in terms of the security policies, processes, organization, and technologies in place. They represent an objective, third-party testament to the security capabilities of Huawei Cloud.

Some of the data security certifications Huawei Cloud has earned are as follows:

- China Ministry of Public Security Graded Protection of Information Security Level-3
- Certification for the Capability of Protecting Cloud Service User Data
- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO 22301
- CSA-STAR Gold
- Payment Card Industry Data Security Standard (PCI DSS)
- China Data Center Alliance (DCA) - Trusted cloud, gold O&M, and five-star cloud hosts

Specifically:

- CSA-STAR Gold

  The CSA STAR gold certification certifies Huawei Cloud's effective management system, a system that systematically and continuously manages security risks and ensures the confidentiality, integrity, and availability of customer data.

- PCI DSS Certification

  Huawei Cloud is the first cloud service provider in China whose platforms and nodes have all earned PCI DSS certification. This certification proves Huawei Cloud's ability to provide customers with financial-grade data security. Customers can deploy financial payment services on Huawei Cloud to achieve compliance with PCI DSS standards during transmission, storage, and processing of payment card user information.

- Certification for the Capability of Protecting Cloud Service User Data

  This certification certifies Huawei Cloud's comprehensive security and privacy protection capabilities.

- ISO/IEC 27018 Certification

  This certification certifies that Huawei Cloud has a comprehensive personal data protection and management system and is a leader in data security management.

  For more information, visit the Huawei Cloud official website and choose **Trust Center** > **Compliance**.

9 Summary

As enterprises are running more and more workloads on the cloud (in terms of both quantity and diversity), protecting data security on the cloud has become a common challenge for both cloud service providers and their customers. Huawei Cloud implements a shared responsibility model for cloud security, where the boundaries of responsibilities are defined clearly for Huawei Cloud and its customers, so the two parties can work together to build a secure and compliant cloud environment. Backed by Huawei's full-stack software and hardware, Huawei Cloud is able to provide reliable, secure cloud services customers can trust to run their enterprise applications.

Huawei Cloud attaches paramount importance to data security. It has built a comprehensive security governance system by aligning itself with international standards, best practices, and relevant capability requirements. Huawei Cloud also lets its customers take advantage of its data protection capabilities built up over the years, enabling them to quickly create new value and accelerate growth.

This white paper shares Huawei Cloud's rich experience in data security with customers and with the industry, with a view to advancing cloud data security in the long run. Moving forward, Huawei Cloud will continue to improve security capabilities and release high-quality cloud services and solutions to help customers create new business value while ensuring compliance with data regulations.

10 Version History

Release On	Version	Description
September 2022	2.0	Regular update
September 2018	1.0	This is the first official release.

