White Paper for HUAWEI CLOUD Data Security

Issue V1.0

Date 2018-09-27

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: http://www.huawei.com

Email: support@huawei.com

Introduction

As cloud computing services continue to develop and mature, an increasing number of businesses and individuals choose to move to clouds. How their data security is guaranteed on clouds becomes their top concern. HUAWEI CLOUD follows the principle of "not accessing customer data without permission."

With this white paper, HUAWEI CLOUD wants to share its data security practices and experience gathered from past years with its customers. Meanwhile, HUAWEI CLOUD is dedicated to improving its data protection capability to help customers achieve greater success with more of its security services.

Contents

1 Ensuring Security While Helping Customers Derive Values from Data

Following the principle of "not accessing customer data without permission", HUAWEI CLOUD has developed a full range of effective data security policies and mechanisms based on its technologies and practices.

- Adhering to the "not accessing customer data without permission" principle

  Customers own and control their data on the cloud. Without their permission, HUAWEI CLOUD will not access any customer data. An example of HUAWEI CLOUD not accessing customer data is the Data Encryption Workshop (DEW) service, which hands keys to customers completely. HUAWEI CLOUD has industry-leading full-stack, full-lifecycle security engineering capability based on full-range software and hardware products. Such capability helps ensure the security of the HUAWEI CLOUD platform and the services it provides.

- Reducing data security risks

  Customers make their own decisions regarding their data security. HUAWEI CLOUD provides a rich variety of services for customers to protect data with. In addition, HUAWEI CLOUD performs continuous and effective security governance centering around security protection, regulatory compliance, and privacy protection in order to ensure that customer data is completely safe.

- Helping customers derive values from data

  In this era of big data, more customers derive greater values from data through data convergence and mining. HUAWEI CLOUD provides multi-dimensional data processing services on its powerful artificial intelligence (AI) and big data platforms. With the authorization from customers, it can help their data yield greater values.

  HUAWEI CLOUD does not access customer data without permission, ensuring that data is owned and used only by customers. To be specific:

  HUAWEI CLOUD does not obtain customer data by any means unless permitted by customers.

  HUAWEI CLOUD will not force any customer to exchange data with itself.

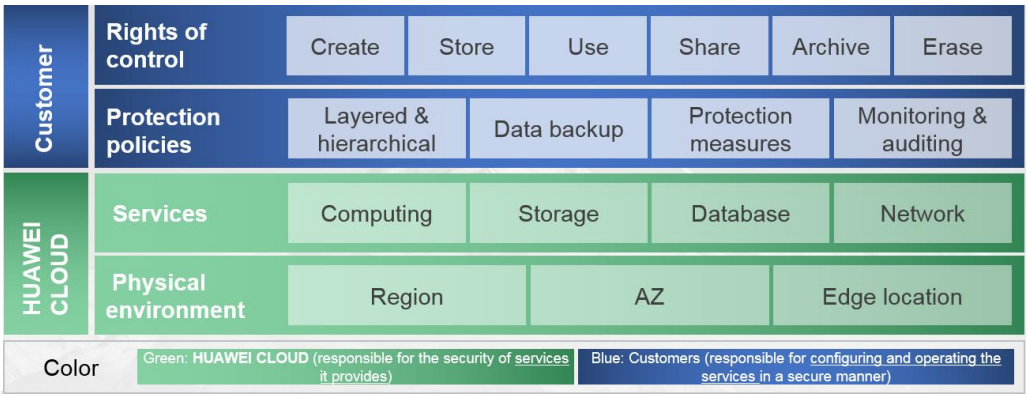
  HUAWEI CLOUD provides AI and big data platforms to help customers derive values from their data.

2 Trustworthy, Open, and Globalized, Enabling Customers to Monetize Data Securely

2.1 Responsibility Sharing and Data Ownership

Responsibility sharing has become a consensus in the industry. HUAWEI CLOUD defines a data security responsibility sharing model based on common industry practices and its specific practices.

Figure 2-1 HUAWEI CLOUD responsibility sharing model



Typically, customers provide or generate the following two types of data:

- Content data

  Content data refers to data stored or processed during the use of HUAWEI CLOUD services, including but not limited to documents, software, images, and audio and video files.

- Account information

  HUAWEI CLOUD collects customers' account information according to applicable laws and regulations. Such information includes but is not limited to registration information and operation logs. For details, see the *Privacy Statement*.

  HUAWEI CLOUD provides data protection services and tools for content data. HUAWEI CLOUD respects and protects account information in accordance with the *Privacy Statement*. It collects as little such information as possible and implements comprehensive measures to protect account security.

- HUAWEI CLOUD responsibilities

As the cloud service provider, HUAWEI CLOUD adheres to its commitment of not accessing customer data without permission and strives to ensure the continuous, efficient, secure, and stable running of the cloud platform. HUAWEI CLOUD provides customers with secure and compliant cloud computing services to enable customers to protect data.

- Customer responsibilities

  As the owners of data, customers shall make data protection policies and take proper measures to ensure data security on the cloud based on their own needs and risks. HUAWEI CLOUD provides data security services and solutions for customers to protect their data with.

2.2 Security Engineering, Regulatory Compliance, Open AI, and Big Data Processing

- All employees of Huawei have their own role to play in ensuring customers' data security

  Cybersecurity and privacy protection are important strategies of Huawei. To ensure the effective implementation of security strategies, the CEO, Board of Directors, and global directors of Huawei personally see through the formulation and publication of its overall cybersecurity strategy, for which all Huawei employees are responsible.

  Based on Huawei's expertise and experience in cybersecurity and privacy protection, a cybersecurity and privacy protection working group has been set up for HUAWEI CLOUD, which reports directly to the CEO. In addition, there is an independent security assessment working group that verifies all services and solutions against cybersecurity and privacy protection requirements. HUAWEI CLOUD's achievements in cybersecurity and privacy protection have been recognized by Deutsche Telekom and passed the Professional Security Auditor (PSA) certification.

- Security engineering is the cornerstone for platform and service security

  HUAWEI CLOUD has industry-leading full-stack, full-lifecycle security engineering capability based on a wide range of software and hardware products. In 2018, HUAWEI CLOUD obtained an excellent result in the assessment performed by the BSIMM. It is the first cloud service provider in China that has ever done that. In addition, it is one of the world's top 3 cloud service providers with respect to security engineering capability.

  In its product development and launch, HUAWEI CLOUD integrates the DevSecOps experience and other industrial standards and practices such as password algorithms, key management, session management, and privacy protection. Security is checked in every phase of product development and launch, from analysis and design, to coding, testing, third-party software management, and launch. This helps HUAWEI CLOUD foster its highly automated capability of software security engineering and a comprehensive tool chain and helps ensure that each service and component meet security requirements.

- Open AI and big data capabilities facilitate customers in deriving values from data

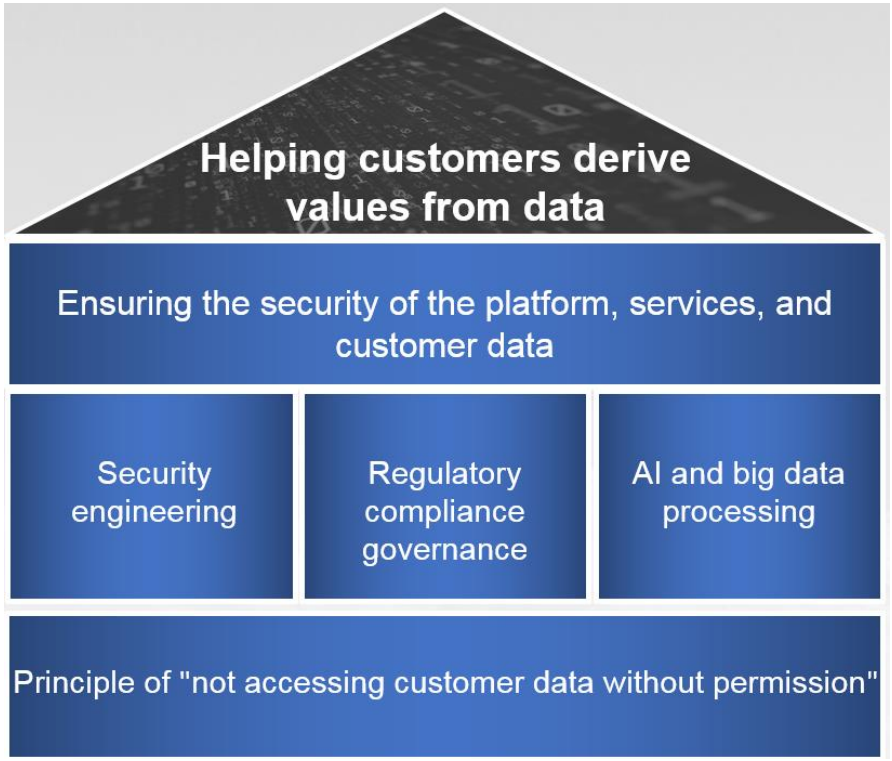
  HUAWEI CLOUD has a wide range of service and solution offerings that can help customers monetize data. For example, the enterprise intelligence (EI) services on HUAWEI CLOUD enable data to create values for customers based on 30 years of expertise in digital technologies. Customers enjoy one-stop network connection and expand their businesses quickly by leveraging Huawei's network resources across the world. HUAWEI CLOUD innovatively provides the DEW service that not only "gives the key to the customer" but also "allows customers to make their own keys", letting customers have full control over their data.

- Regulatory compliance governance helps continuously ensure data security

  On HUAWEI CLOUD, we build a data security governance system that integrates prediction, protection, detection, and response abilities. The system performs cybersecurity governance centering around security protection, regulatory compliance, and privacy protection. It ensures the security of data on the cloud by continuously monitoring and analyzing risks, intelligently combining multiple security mechanisms, and promptly updating security policies, processes, and technologies.

  HUAWEI CLOUD complies with international standards and implements global compliance governance. To help customers meet security regulations, HUAWEI CLOUD provides best practices and, through regulatory compliance services, security hardenings and emergency responses.

Figure 2-2 HUAWEI CLOUD data security assurance system



3 Industry-leading Security Engineering and Trustworthy Platform and Services

3.1 Full-Stack, Full-Lifecycle Security Engineering Capability Based on a Wide Range of Software and Hardware Products

HUAWEI CLOUD provides full-stack protection from the chip to the cloud, including the chip, systems, platform, applications, and data. The chip uses a self-developed, proprietary security protocol and the trusted computing technology to offer solid protection from the bottom.

Security-related actions are performed throughout the lifecycle of a service, including security design, coding, testing, acceptance, release, and vulnerability management, in order to ensure service and product security.

A security lab is set up to conduct a stringent, risk-based security test on products to continuously improve the security of the platform, services, and components. Products cannot be launched without passing the test.

To ensure that HUAWEI CLOUD and services it provides meet local laws and regulations, and customers' security requirements, Huawei relies on its in-house privacy and cybersecurity team, and best third-party counsels to track, analyze, and research related laws and regulations and technical requirements, and implement the requirements throughout the product lifecycle, including R&D, rollout, and O&M, to safeguard the interests of customers.

3.2 Building a Full-Stack Data Security System

Huawei has invested heavily in security R&D, and has developed and innovated security protection technologies in the fields of chips, platforms, systems, applications, and data. Huawei aims to build a full-stack and in-depth security system to ensure customer data security.

- Secure encryption and chip-level trusted computing

  Huawei has profound technical accumulation in the trusted computing field, and pioneers in launching a trusted server and a trusted cloud platform solution that supports the national encryption algorithm. Based on the trusted computing module chip, HUAWEI

CLOUD can measure the integrity of cloud hosts and provide more security features to meet higher security requirements, reducing the risks of software and hardware being tampered with.

With the Intel SGX technology, HUAWEI CLOUD build up the chip-level and lightweight capabilities of key management and data encryption. As a result, the dependency on traditional Hardware Security Modules (HSMs) is eliminated. Furthermore, high-performance encryption and decryption are guaranteed in the chip-level security environment, which effectively reduces the risk of plaintext memory leakage and ensures data security in transit.

- Platform

  The HUAWEI CLOUD Unified Virtualization Platform (UVP) runs on physical servers. It abstracts physical resources of servers, and builds multiple isolated VM environments running on a single physical server. UVP provides the virtualization capability based on the hardware-assisted virtualization technology, providing an efficient running environment for VMs and ensuring that VMs run in a valid space. This prevents VMs from initiating unauthorized access to the UVP or other VMs.

- System

  Huawei's EulerOS has passed the level-4 certification of information security technology required by the Ministry of Public Security. EulerOS integrates advanced Linux technologies and optimizes CPU scheduling, memory, network, and storage to help customers achieve effective resource restructuring and provide customers with a competitive open IT platform. The system is easy to use, and provides high performance, stability, availability, and scalability, catering for customer's increasingly complex and changeable service requirements. EulerOS also provides configurable policies for security hardening as well as OS security capabilities at kernel level, which can effectively prevent intrusions and ensure system security.

- Application

  With industry-leading security engineering capabilities, HUAWEI CLOUD provides systematic and strict security control over the entire process of application development, and ensures that applications meet security requirements. Huawei's proprietary API gateway enables applications to provide standard and integrated APIs for customers. These APIs offer security capabilities such as identity authentication, transmission encryption, and fine-grained traffic control, preventing data theft and sniffing. In addition, HUAWEI CLOUD leverages technologies such as deep learning, runtime application protection, and decentralized authentication to further build advanced security capabilities, such as user behavior profiles and service risk control, to monitor and intercept abnormal behaviors in real time, and ensure secure and stable running of application services.

- Data

  HUAWEI CLOUD applies Huawei's accumulated experience in information asset protection to cloud services, in order to build the capabilities to protect data throughout the full lifecycle. Through intensive R&D in technologies, such as automatic sensitive data discovery, dynamic data anonymization, high-performance and low-cost data encryption, abnormal operation audit, and data destruction security, HUAWEI CLOUD implements data management and control in all aspects, such as creation, storage, use, sharing, archiving, and destruction, thereby ensuring cloud data security.

3.3 Managing Data Security Throughout the Lifecycle

HUAWEI CLOUD has complete systems, processes, automated platforms, and tools for end-to-end lifecycle management of software and hardware. A full lifecycle includes the following phases: security design, security coding and testing, security acceptance and release, and vulnerability management.

Security design

Products and components of HUAWEI CLOUD services comply with Huawei's security design principles, specifications, and baselines. During security requirement analysis and design, threat analysis is performed based on service scenarios, data flow diagrams, and networking models, with highly automated tools and rich set of cases. As a result, the efficiency and integrity of solution design are optimized. Data security practices in the design are described as follows:

- Data isolation

  HUAWEI CLOUD houses data of numerous customers. At the planning stage of each product or component, isolation mechanism is integrated to prevent unauthorized access and tampering, and to reduce data leakage risks.

  For example, data isolation is an important feature of HUAWEI CLOUD's storage services such as Elastic Volume Service (EVS), Object Storage Service (OBS), and Scalable File Service (SFS). For block storage, data storage is isolated by volume (EVS disk). Each volume is associated with a customer ID. The VM to which the volume is attached must have the same customer ID, ensuring absolute data isolation for customers.

- Data encryption

  HUAWEI CLOUD services are integrated with DEW to facilitate key management for customers who can easily store and encrypt data, with only simple encryption configurations. Currently, DEW supports services such as OBS, EVS, Image Management Service (IMS), RDS, and SFS. The number of supported services is increasing, greatly facilitating customers in terms of data encryption.

  Customers can access HUAWEI CLOUD services through the management console or APIs. Security transmission protocols are used to ensure secure transmission channels, which effectively reduce the risk of malicious sniffing during data transmission over networks.

- Data redundancy

  Data storage in HUAWEI CLOUD uses the multi-copy backup and erasure code (EC) design. With the redundancy and verification mechanisms, damaged data can be quickly detected and restored. This ensures that services are not interrupted even if some physical devices are faulty. HUAWEI CLOUD data storage durability reaches the industry-leading level. For example, the data durability of OBS is up to 99.999999999% (11 nines).

- Privacy protection design

  HUAWEI CLOUD services are designed in compliance with the *Privacy Protection Design Specifications*, which specifies privacy baselines, maintains privacy integrity, guides through the privacy risk analysis.

Security coding and testing

HUAWEI CLOUD strictly complies with the security coding standard of programming languages released by Huawei. R&D personnel must learn the coding standard and pass the examination before work on the position of programming. Static code scanning tool is used to

perform routine check in the cloud. The check result is stored in the cloud service tool chain, for later evaluation of code quality. Before releasing a cloud service, all static code scanning alarms must be cleared. By doing so, coding-related security issues are effectively controlled during the rollout of the service.

Security requirements identified in the design phase, penetration test cases from the attacker's perspective, and industry standards are used as check items, based on which security test tools are developed. Before a service is released in the cloud, multiple rounds of security tests are performed, ensuring that the service meets the security requirements.

Security acceptance and release

Release of an important cloud service or version requires the Global Cyber Security & Privacy Officer (GSPO) and Chief Legal Officer (CLO) approvals. Strict reviews are conducted to analyze the compliance requirements of all service areas, ensuring that HUAWEI CLOUD services are in compliance with the laws and regulations.

Vulnerability management

HUAWEI CLOUD builds a complete vulnerability management system to track and manage all processes, such as vulnerability awareness, vulnerability disposal, and vulnerability disclosure, to ensure that vulnerabilities of products and components in the cloud can be detected and rectified in a timely manner, reducing the risks caused by malicious exploitation of vulnerabilities.

3.4 Managing the Security of Open-Source and Third-Party Software from End to End

To provide customers with various cloud service products and build a sound ecosystem, cloud service providers introduce a lot of open-source and third-party software. HUAWEI CLOUD implements strict requirements on introduction of open-source and third-party software, ensuring secure introduction and use.

HUAWEI CLOUD has clear security requirements and complete process control for introducing open source and third-party software. The following aspects are strictly managed and controlled: sourcing analysis, security testing, code security, risk scanning, legal review, application for software, and software decommissioning. For example, during sourcing analysis, the cyber security evaluation requirements for the open-source software selection is added to control the process.

In practice, if a piece of third-party software is used as a part of the service or solution, the integration points between open-source (or third-party) software and HUAWEI CLOUD software must be evaluated. If independent third-party software is used in the solution, whether new security issues are introduced must be evaluated.

HUAWEI CLOUD provides network security capabilities to the community. When an open-source vulnerability occurs, HUAWEI CLOUD can use its influence in the community to discover and fix vulnerabilities at the earliest moment. During vulnerability response, open-source and third-party software must be tested as part of services and solutions to verify whether known vulnerabilities are fixed. The list of fixed vulnerabilities must be published with the release notes.

4 Helping Customers Securely Derive Value from Data Using Our AI and Big Data Platforms

4.1 Sharing 30 Years' Digital Technologies to Help Customers Derive Value from Data

HUAWEI CLOUD EI provides an open, reliable, and intelligent platform based on AI and Big Data technologies. It enables enterprise application systems to view, listen, and speak based on industry scenarios, and equips the systems with the ability to analyze and understand images, videos, speech, and text. In this way, more enterprises have access to AI and Big Data services, scenario-specific solutions, and EI intelligent twins. It greatly accelerates service development and benefits the society. HUAWEI CLOUD EI provides intelligent cloud services including Essential Platform, Big Data, video services, Speech and Semantics, Visual Cognition, and Industry Scenario Solutions.

The Essential Platform services launch Deep Learning Service (DLS), Deep Learning HMI, and Graph Engine Service (GES) featuring powerful machine learning, deep learning, and relationship analysis capabilities. In General Services, Visual Recognition lately launches Face Recognition, Image Recognition, and Content Moderation services, extending the application of computer vision. The newly released Speech and Semantics services such as Automatic Speech Recognition, Text To Speech, Natural Language Processing, and Question Answering Bot, enable natural language input and man-machine interaction. EI Intelligent Twins in Industry Scenario Solutions include Intelligent Water, Intelligent Manufacturing, Intelligent Power, Intelligent Transportation, Intelligent Finance, and Intelligent Retail.

4.2 Protecting Data Layer by Layer to Ensure Full-Lifecycle Data Security

HUAWEI CLOUD provides full-lifecycle data protection, which enables customers to safely process data on the cloud. The operation interfaces are friendly for users and meet customized data security requirements in different industries.

Figure 4-1 Key protection measures in different phases of data lifecycle

4.3 Classifying and Isolating Data to Guarantee a Good Start in Data Creation

Data creation indicates generating new content or replacing, updating, or modifying existing content. It is recommended that customers classify data, analyze risks, and then choose storage location, storage service, and security protection measures for the data based on the risk analysis results. In this way, data is classified and isolated at the beginning of its lifecycle.

Key Capabilities

- Autonomous Location Selection

  HUAWEI CLOUD provides services by regions where customers' data is stored. Without authorization, HUAWEI CLOUD never moves customers' data across regions. When using cloud services, customers can select regions for data storage based on the proximity access principle and laws and regulations of different regions.

- Isolated Environment Construction

  When customers use services such as EVS, OBS, RDS and Cloud Container Engine (CCE), HUAWEI CLOUD uses access control mechanisms such as volumes, buckets, database instances, and containers to ensure that customers can access only their own data. In scenarios where customers build on-premises storage device, if, for example, installing database software on virtual machine instances is required, customers are recommended to use HUAWEI CLOUD VPC to build a private network. Then customers can divide the network by planning subnets and configuring routing policies and place storage resources on an internal subnet. In this way, customers can strictly control the ingress and egress traffic of the subnet and VMs by configuring the network ACLs and relevant rules.

Related Services

- EVS
- OBS
- RDS for MySQL

4.4 Dynamically Protecting Data to Minimize Storage Risks

Data storage refers to submitting data to a certain repository, which occurs usually when data is created. For sensitive and important data stored on the cloud, customers are advised to encrypt it to prevent data leakage.

Key Capabilities

- Storage Encryption

  HUAWEI CLOUD encapsulates complex data encryption and key management logic to simplify encryption process for customers. Currently, services including EVS, OBS, IMS and RDS provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms.

  The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD DEW, which provides full-lifecycle key management. Without authorization, others cannot obtain keys to decrypt data, which ensures data security on the cloud. DEW adopts the layered key management mechanism. Specifically, after association configuration on DEW Console or using APIs, customer's master key stored in DEW encrypts the encryption keys of each storage service, while the master key is encrypted by the root key stored in HSM. In this way, a complete, secure and reliable key chain is formed. HSM is certified by international security organizations and can prevent intrusion and tampering. Even Huawei O&M personnel cannot obtain the root key. DEW also allows customers to import their own keys as master keys for unified management, facilitating seamless integration with customers' services.

  Customers can use the Dedicated HSM service of HUAWEI CLOUD when they are accustomed to use traditional physical cryptographic machines or have higher compliance requirements. Dedicated HSM provides customers with CSCA (China State Cryptography Administration) certified HSMs or FIPS 140-2 validated level-3 HSMs or their virtualization instances to meet customers' higher security requirements.

- Storage Disaster Recovery Service (SDRS)

  For enterprises, the Disaster Recovery (DR) mechanism is indispensable to ensure the continuity of services in the event of disasters. The DR system consists of network, application, data and other layers. The data layer focuses on maintaining data consistency and reducing the data loss rate, which is vital to the DR system. SDRS of HUAWEI CLOUD provides disaster recovery capabilities for ECS, EVS, and Dedicated Enterprise Storage Service (DESS). It provides VM-level disaster recovery protection across AZs by using technologies such as storage replication, data redundancy, and cache acceleration. When a production site is faulty, customers can quickly recover services at the DR site through simple configurations, ensuring data reliability and service continuity.

Service Resources

- DEW
- SDRS

4.5 Effectively Controlling Data Usage

Data usage indicates viewing, processing, or accessing data except for modifying it. In the Big Data era, enterprises strive to create more value through data convergence and mining, which also poses data leakage and law violation risks. To avoid these risks, HUAWEI CLOUD provides customers with services in data access control, security protection, and auditing to help them control data usage and transfer in a fine-grained manner.

Key Capabilities

- Access Control

  Identity and Access Management (IAM) provides customers with user account management, identity authentication, and fine-grained cloud resource access control that are suitable for enterprises. IAM provides the Multi-factor Authentication (MFA) function to improve the security of account login and important operations. IAM supports the digital signature and timestamp mechanisms to prevent tampered API requests and replay attacks. IAM supports federated identity authentication with customer's account management system, allowing users to access HUAWEI CLOUD after being authenticated in the account management system.

  Malicious operations or misoperations from O&M engineers are more destructive to the system because these personnel have high permissions and are more likely to operate raw data. Therefore, it is recommended that customers use the Cloud Bastion Host (CBH) service to control O&M activities. CBH provides one-stop services including account and asset management, access control, and operation auditing to help customers control O&M and audit regulatory compliance.

- Database Security Protection

  Customers can use HUAWEI CLOUD Database Security Service (DBSS) to protect databases. With the patented reverse proxy and machine learning technologies, DBSS provides such functions as data masking, database firewall, and database auditing to ensure data security on the cloud. DBSS can identify sensitive data based on rules and hide sensitive data from unauthorized users in real time based on masking policies, which neither affect database performance nor change the original storage. As a database firewall, DBSS can monitor and intercept malicious attacks such as SQL injection in real time, improving the database resilience.

- Object Storage Watermarking

  When customers need to protect data copyright, authenticate data, or trace data, they can choose the digital watermarking technology. HUAWEI CLOUD OBS is able to add text or image watermarks to images. Users can set watermarks for images on the OBS Console or through code editing or interface invoking, and quickly obtain the processed images.

- Auditing

  For such services as OBS and SFS, Cloud Trace Service (CTS) can record customers' operations on data. For RDS, DBSS is able to provide database column-level management and access activity records. For customized log collection requirements, Log Tank Service (LTS) collects any text logs and provides unified management, supporting data query from billions of data records in mere seconds.

Related Services

- IAM
- CBH
- DBSS

- CTS
- LTS

4.6 Strict Management and Control to Ensure Data Sharing Security

Data sharing indicates exchange of data between users, customers, and partners. Opening and sharing data is the prerequisite for data convergence and mining, which can eliminate information silos and derive more value from data. To ensure data security, customers are advised to strictly control data access and transmission.

Key Capabilities

- Access Control

  IAM supports resource sharing among accounts by creating agencies. Using IAM, customers can create an agency and grant resource management permissions to the delegated account. Then the delegated account can log in to HUAWEI CLOUD and manage shared resources. Customers do not need to share security credentials with the delegated account. In this way, resources can be shared with account security protected.

- Transmission Encryption

  When customers provide web services through the Internet, they can use the SSL Certificate Manager (SCM) service jointly provided by HUAWEI CLOUD and world-renowned Certificate Authorities (CAs). By applying for and configuring certificates for websites, customers can identify trusted websites and ensure secure transmission using encryption protocols.

  For customers' services concerning hybrid cloud deployment and global layout, services including Virtual Private Network (VPN), Direct Connect and Cloud Connect are provided by HUAWEI CLOUD to achieve interconnection among services and secure data transmission between different areas.

  VPN uses Huawei-proprietary hardware to virtualize private networks on the Internet based on IKE and IPsec. Secure and reliable encrypted transmission channels are established between the local data center and HUAWEI CLOUD VPC and between VPCs in different regions of HUAWEI CLOUD.

  Based on carriers' private line networks, the Direct Connect service provides a dedicated encrypted transmission channel between the local data center and HUAWEI CLOUD VPC. Private lines of different customers are physically isolated to meet higher security and stability requirements.

  The Cloud Connect service is a one-stop cloud connection network service based on Huawei's years of global IT operation experience and network resource layout in many countries and regions. It can quickly establish a private communication network between multiple local data centers and VPCs. Cross-cloud VPC interconnection is supported, greatly improving the security and speed of customers' global service expansion.

Related Services

- SCM
- VPN
- Direct Connect
- Cloud Connect

4.7 Archiving by Category for Effective Data Backup and Restoration

Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Data backup, archiving, and quick recovery capabilities are critical for enterprises. In case of accidents such as misoperations, faults, network attacks, and disasters, these capabilities can help restore data in time to avoid data loss and ensure service continuity.

Key Capabilities

- **Backup and archiving**

  HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in specific scenarios. Customers can use the versioning function of OBS, Volume Backup Service (VBS), and Cloud Server Backup Service (CSBS) to back up in-cloud documents, disks, and servers. Benefiting from on-demand use, scalability, and high reliability features of cloud services, customers can also use the Backup and Archive Solution, backup and archiving software, and HUAWEI CLOUD infrastructure to back up on-premises data to HUAWEI CLOUD.

  With the DEW service, customers can encrypt backup data easily and quickly, thereby ensuring data security.

- **Recovery drill**

  To improve the emergency response capability, customers can perform the recovery drill periodically. The Backup and Archive solution allows customers to use backups to restore data in the in-cloud system. After the data is restored, resources can be released, significantly reducing the recovery drill cost.

Related Services

- DEW
- VBS
- CSBS
- Backup and Archive

4.8 Permanently Destroying Data to Ensure that Data Is Completely Cleared

Data destruction is the process of destroying data stored on tapes, hard disk, and other forms of electronic media so that it is completely unreadable. If customers want to delete data or data needs to be deleted due to the expiration of a service, HUAWEI CLOUD strictly follows the data destruction standard and agreement with customers to clear the stored data. Data destruction and accidental deletion may lead to data unrecoverable or data loss. Therefore, it is recommended that you back up (for details, see section 4.6 "Strict Management and Control to Ensure Data Sharing Security") or migrate the data before destroying it.

Key Capabilities

- **Migration of content data**

  The Cloud Data Migration (CDM) service enables data migration among multiple types of data sources, such as databases, data warehouses, and files, and supports data

migration across multiple environments, such as data migration to the cloud, data exchange in the cloud, and data migration to on-premises data centers.

- **Destruction of content data**

  During the destruction of customer data, HUAWEI CLOUD clears the specified data and all the copies. Once customers agree the deletion, HUAWEI CLOUD deletes the index relationship between customers and data, and clears the storage space, such as memory and block storage before reallocation, to ensure that related data and information cannot be restored. If a physical storage medium is to be disposed, HUAWEI CLOUD clears the data by degaussing, bending, or breaking the storage medium to ensure that data on the storage medium cannot be restored.

- **Deregistration**

  HUAWEI CLOUD allows customers to deregister accounts. After customers' application for account registration is approved, their content data enters the retention period. Within the retention period, customers cannot access or use the cloud service, but data stored in the cloud service remains. After the retention period expires, data stored in the cloud service will be deleted and cannot be restored.

Related Services

CDM

5 Implementing Global Regulatory Governance to Ensure Data Security

5.1 Security Governance and Dynamic Collaboration to Ensure In-Cloud Data Security

Huawei has built a cloud data security system that integrates prediction, protection, detection, and response capabilities. The system, together with scenario-oriented defense measures, ensure data security on the cloud.

Figure 5-1 Key protection measures

Prediction

A uniform analysis and alert platform is designed for customers to understand the overall data security posture, quickly identify and respond to security events, and perform risk assessment and security posture prediction by analyzing correlations among alarms, events, and assets. In this way, protection policies can be generated in advance to prevent potential risks.

A complete vulnerability management system is built to track and manage the whole process ranging from vulnerability awareness, vulnerability disposal, to vulnerability disclosure. This

can ensure that vulnerabilities exposed to service products and components on the cloud platform are detected and fixed at the earliest moment and reduce the risks due to malicious exploitation of vulnerabilities.

Protection

- **Physical and environmental security protection**

  Strictly following the international and national standards, HUAWEI CLOUD carries out site selection, design, and construction of data centers (DCs), and implements hierarchical security protection for data centers, from the fence to the DC building, and from the DC building to modules, from modules to cabinets, from cabinets to servers, to ensure the physical and environmental security of cloud DCs. In the meantime, 24x7 monitoring is enabled to detect and eliminate potential risks to ensure stable running of DCs.

- **Network security protection**

  HUAWEI CLOUD helps customers build a network security protection system to prevent data from being stolen or disclosed.

  HUAWEI CLOUD deploys Anti-DDoS devices at the Internet border to detect and clean abnormal and ultra-large traffic attacks. Intrusion prevention devices are deployed at the border of key network zones to identify attacks from the Internet and customers and automatically block these attacks.

  All hosts on the cloud platform are installed with the security protection software for weak password detection, configuration management, intrusion detection, and emergency response to build a compliant and secure host environment.

  Web security protection devices are used to defend against application-layer attacks, ensuring web service security.

- **O&M management**

  HUAWEI CLOUD develops and implements strict standards, processes, and control measures to implement uniform access, authentication, authorization, and audit for O&M operations.

  O&M personnel pass the two-factor authentication, access the O&M environment, and then switch from the bastion host to the target host. The password of the target host is reclaimed by the bastion host and updated periodically so that the O&M personnel do not need to obtain the password. Strict access to the O&M environment blocks unauthorized internal access and protects data security.

  HUAWEI CLOUD implements role-based access control for O&M personnel. Minimum permissions and strict behavior audit ensure that O&M personnel do not access customers' data.

- **Detection**

  HUAWEI CLOUD analyzes alarm information of each security device and builds models based on machine learning technologies and expert experience to detect unknown data security threats and take effective measures to defend against the threats.

  In compliance with national laws and regulations, HUAWEI CLOUD has built a centralized and comprehensive log auditing system. O&M operations of internal personnel are collected and recorded by the log platform. The log auditing system provides powerful data storage and query capabilities to ensure that all logs can be stored for more than six months. HUAWEI CLOUD also sets up an internal audit department to regularly audit the activities during O&M, thereby detecting and correcting violations in a timely manner.

- **Response**

Adhering to the rapid detection, impact scoping, isolation, and recovery principles, HUAWEI CLOUD responds to events based on the consequences of security events on the entire network and customers. A professional response team and expert resource pool are ready to help 24x7. In accordance with related laws and regulations, HUAWEI CLOUD provides timely disclosure of related events, notifies customers promptly, and implements emergency plans and recovery processes to minimize service impact.

5.2 Adherence to International Data Security Compliance Certifications and Standards

Contributing to best practices and years' experience in data protection, HUAWEI CLOUD plays an active role in the establishment and certifications of industry-wide data and privacy protection standards. On the one hand, certifications and reports allow customers to verify the effectiveness of HUAWEI CLOUD security measures. On the other hand, HUAWEI CLOUD shares security protection practices and experience with customers, helping them protect in-cloud data security.

To date, HUAWEI CLOUD has obtained the following security certifications:

- China Graded Information Security Protection Grade IV
- Certification for the capability of protecting cloud service user data (trusted cloud)
- ISO/IEC 27001
- ISO/IEC 27017[1]
- ISO/IEC 27018
- ISO 22301[2]
- CSA STAR Gold Certification
- Payment Card Industry Data Security Standard (PCI-DSS)
- China Data Center Alliance (DCA) Trusted Cloud Services (TRUCS) Certification, Gold O&M, and Five Star Certification (the highest evaluation standard) for HUAWEI CLOUD ECSs
- Trusted Cloud (Germany)[3]
- TÜV Trusted Cloud (Germany)[4]
- TCDP (Germany)[5]
- The following certifications are used as examples to describe that how HUAWEI CLOUD complies with data security standards.

- **CSA STAR Gold Certification**

  CSA STAR Gold Certification demonstrates that HUAWEI CLOUD has established a scientific and effective management system that can systematically and continuously manage security risks and ensure data confidentiality, integrity, and availability of itself and customers.

- **PCI DSS certification**

  HUAWEI CLOUD is the first cloud service provider in China that has passed the PCI DSS certification for all platforms, nodes, and services. This certification proves that HUAWEI CLOUD can provide financial-level data security for customers so that customers can deploy financial payment services on HUAWEI CLOUD and achieve security compliance during transmission, storage, and processing of card information.

- **Certification for the capability of protecting cloud service user data (trusted cloud)**

With the comprehensive security protection capabilities and data protection mechanism, HUAWEI CLOUD became one of the first cloud service providers that obtained the certification for the capability of protecting cloud service user data.

- **ISO/IEC 27018 Certification**

  This certification demonstrates that HUAWEI CLOUD has established a complete personal data protection management system and is in the global leading position in data security management.

5.3 Strictly Protecting Account Information

HUAWEI CLOUD understands and respects customers' rights to their account information, makes due technical efforts, and takes stringent management measures to ensure account security. When processing account information, HUAWEI CLOUD strictly complies with relevant laws and regulations and refers to industry best practices.

HUAWEI CLOUD processes customers' account information only in the following situations:

- Provide services for customers according the *HUAWEI CLOUD User Agreement*, *Privacy Statement*, and other cloud service agreements signed by customers.
- Required by the applicable laws and regulations or competent authorities.

HUAWEI CLOUD requires that the personnel who are responsible for processing account information must sign a confidentiality agreement before on-boarding and strictly control access to and record operation logs to establish a data security mechanism throughout the pre-event, in-event, and post-event phases.

HUAWEI CLOUD respects and protects the legitimate rights and interests of customers as data subjects for their account information, including the rights to know, and access, modify, and delete data. HUAWEI CLOUD endeavors to meet the preceding right requirements.

6 Conclusion

With cloud computing growing faster than ever, more and more enterprises choose to migrate their services to the cloud, which puts more pressure on data security. To tackle the complex and changeable network environment and security challenges, HUAWEI CLOUD vows not access user data, conforms to the shared responsibility model, and makes the most of the full-stack technological advantages to build trusted cloud services and enhance data security with customers.

Putting data protection as the top priority and security engineering as the cornerstone, HUAWEI CLOUD offers full-stack security and protect products and services throughout their full lifecycle. Led by the regulatory governance, HUAWEI CLOUD conforms with internationally accepted standards and capabilities requirements to build a sound security governance system so that customers can carry out services on HUAWEI CLOUD with no worries. In addition, Huawei opens up the AI and big data platforms for customers to get the most of them, building lasting and win-win relationships with customers.

Given this opportunity, we share HUAWEI CLOUD's extensive experience in data security with our customers and partners to promote progress in the cloud data security field. HUAWEI CLOUD will make constant efforts to improve security protection capabilities and deliver high-quality cloud services and solutions to help customers achieve business success.

A Change History

Release On	Version	Description
September 2018	1.0	This is the first official release.

B References

[1] Open Telekom Cloud by Deutsche Telekom (DT) in partnership with Huawei has achieved ISO/IEC 27017 certification.

[2] Open Telekom Cloud by DT in partnership with Huawei has achieved ISO 22301 certification.

[3] Open Telekom Cloud by DT in partnership with Huawei has obtained the Trusted Cloud Service certificate.

[4] Open Telekom Cloud by DT in partnership with Huawei has obtained the TÜV Trusted Cloud certificate.

[5] Open Telekom Cloud by DT in partnership with Huawei has obtained the Trusted Cloud Data Protection Profile (TCDP) certificate.

