

Tencent Cloud Security White Paper

June 2019

Tencent Cloud Security Team & Tencent Research Institute Security Research
Center

Tencent Cloud




腾讯云

【Copyright Notice】

©2019-2021 Tencent Cloud. All rights reserved.

The copyright of this document belongs to Tencent Cloud. No part of this document may be copied, modified, plagiarized or distributed in any form, without prior written permission of Tencent Cloud.

【Trademark Statement】

 Tencent Cloud and other trademarks related to Tencent Cloud Services are the properties of Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliates.

All trademarks of third-party entities involved in this document are legal property of their respective owner.

【Service Statement】

This document is for reference only. Tencent Cloud makes no warranties, explicit or implied, regarding the information in this document. This document is based on the status quo. The information and opinions contained in this document, including the website and other Internet website references, are subject to change without notice. You bear the risk of using it.

This document does not grant you any legal rights to Tencent products intellectual property. You may copy and use the document contents for your internal reference purposes.

Examples in the document are made-up examples and are for illustrative purposes only. No factual association or connection can be deduced or anticipated based on examples.

Tencent Cloud: Secure & Reliable

Preface

Cyberspace is changing rapidly and each year brings us some new trends. Internet of Things and Cloud extended the two-dimensional space to four-dimensional space, so security is not only a technological concern, but an issue of the entire industry.

From a security perspective, damage from attack and information loss in the Cloud can be dozens or even hundreds of times than that of before. Technologies that positively impact production also let attackers get past detection. Dark web exploits Cloud technology, and attackers are seeking vulnerabilities and methods of attack as everything gets more interconnected. From a protection perspective, smart cloud security is inevitable due to the convergence of big data, AI and cloud computing. Real-time analysis and smart decision-making are now realities thanks to the development of massive data archiving, cloud computing resources, and AI analytic algorithms. Burgeoning cloud technologies are creating smarter and stronger security protection.

Tencent Cloud is a major player of cloud computing in China and we care a lot about security. We have proposed a strategic plan called the "Tencent Cloud smart security solution: a collaboration of cloud, client, and channel". Tencent Cloud also collaborated with partners and built a smart and safe cloud environment.

Full-link products and engines are the foundations of smart security. Full-link product coverage and data information flow are essential to building smart security, and Tencent has its advantages. We witnessed the opportunity to build a security system when companies migrated to cloud using cloud as the platform and channel. We try to build a cooperative defense and control system based on cloud, channel, and client integration. Additionally, we try to deliver security services as well as Cloud defense products and solutions.

The complex global environment brought unprecedented security challenges to various industries, and it is a common consensus to pursue independence as well as cooperation. So, cloud security collaboration is still important in the digital economy. Additionally, cybersecurity is a difficult job as it is easier to attack than defending, and no company can manage it alone. From past lessons, we understand cross-industry cooperation is important for now and the future.

Speaking from a security perspective and past experience, controlling key areas is effective and necessary. A multi-dimensional cyberspace requires a defense system that is also multi-dimensional. As network is composed of many parts, Tencent Cloud will work with industry partners to build a safer environment.

Tencent was established two decades ago, and has gained strong technical and security capabilities. We are one of the earliest companies that focuses on cloud computing environment security. Tencent Cloud is trying to offer a secure, reliable and smart cloud based on cloud, channel, and client integration so that companies can thrive and stay secure in the digital age.

Smart Security

Smart Security is analyzing and processing security data using Tencent security technologies. Smart security can effectively prevent security threats, and even actively eliminate threats all together to help partners and companies with different digitalization security requirements. Solutions based on smart security can improve companies' security and threat response abilities, so that customers can focus on their business and future development. Additionally, smart security promotes the development of the entire security environment.

We stick to our sharing, developing and win-win principle and work with individuals, security vendors, companies, and countries to create a secure environment and contribute to enterprise security. **Sharing refers to sharing basic security data, which is the basis of the entire security environment.** All parties will stick to the openness and sharing principle, and share insensitive basic security data with other parties for security development. **Developing refers to building a secure environment together.** Building a secure environment is all parties' common goal and responsibility. The secure environment we are trying to create is built by us, our partners as well as customers, and we will try our best to support and protect the security environment. **Win-win is common good for all parties.** Building a security environment is not a zero-sum game, and we want common good for all parties. The ultimate goal is to build a cyberspace that is safe, peaceful and beneficial, and benefit partners, corporate customers, countries and the entire society.

Smart security not only is defensive, but can also predict risks, detect unknown threats and security problems, and assist decision-making and security collaboration. Individuals, companies, countries and society can effectively address challenges and adapt to security trends with smart security and company security solutions for cloud, channel, and client.

In terms of management, smart security lowers companies' security management and operation personnel requirements., and brings security experts together and solves company's security talents shortage. For companies, security management and operation staff only need to understand the management and operation of smart security to prevent accidents and reduce loss. Because labor and security costs are cut down, more resources can be invested to the company's main business, which improves product quality and competitiveness. It is also beneficial to innovation of the industry and the entire society.

In terms of technology, smart security will fully integrate hardware and software resources, provide continuous services, and have core security capabilities such as threat awareness, risk trend prediction, intelligent decision-making, and security collaboration. Smart security enterprise security solutions will solve the limitations of traditional protection methods. Intelligent analysis and prediction will find threats that cannot be identified by traditional characterization methods, prevent and block cyber threats, and even proactively kill threats.

In terms of products, smart security offers an enterprise security solution covering cloud, channel, and client. Interconnected security products and shared security data strengthen

the weak links of enterprise security management and forms an overall defense system. Connected “cloud, channel, client” products make security solution more integrated rather than isolated, which assists company event security protection, adapts to the trend of connected security products, and improves company's overall security level.

Tencent, our partners and customers work together using smart security to share security information, and build a secure and harmonious cyberspace. We hope that we can contribute to company security building, solve company security challenges, adapt to company security trends, and ultimately achieve a win-win for all.

TABLE OF CONTENTS

1. OVERVIEW	10
2. CLOUD SERVICE TYPE.....	13
3. THE SECURITY RESPONSIBILITY SHARING MODEL.....	17
4. RISK AND COMPLIANCE	22
4.1 Industry Cloud Certification System	23
4.2 Security compliance.....	27
4.3 Security Compliance Service	29
4.4 Privacy Protection	30
5. IT INFRASTRUCTURE SECURITY	31
5.1 Physical Security.....	32
5.2 Network Security	34
5.3 Customer-oriented Basic Cloud Products	37
6. DATA SECURITY	45
6.1 Secure Data in Cloud	46
6.2 User Data Protection Practice	48
7. OPERATION MANAGEMENT SECURITY	51
7.1 Tencent Cloud's Operational Management Capabilities	52
7.2 Customer-facing Operational Management Products	55
8. TENCENT CLOUD SECURITY ENVIRONMNET	59
8.1 Internal Environment - Resource Integration, "Cloud, Channel, Client" Security System Establishment.....	60
8.2 External Environment - Cooperation with Multiple Parties to Establish an Open, Coordinated and Win-Win Security Environment	63

APPENDIX	64
----------------	----

1. Overview

Tencent Cloud has provided cloud products and services to millions of companies and developers for their development demands in games, video, mobile, healthcare, government, finance and other Internet-related industries.

Below is the overall Tencent Cloud production framework based on years of business practice:

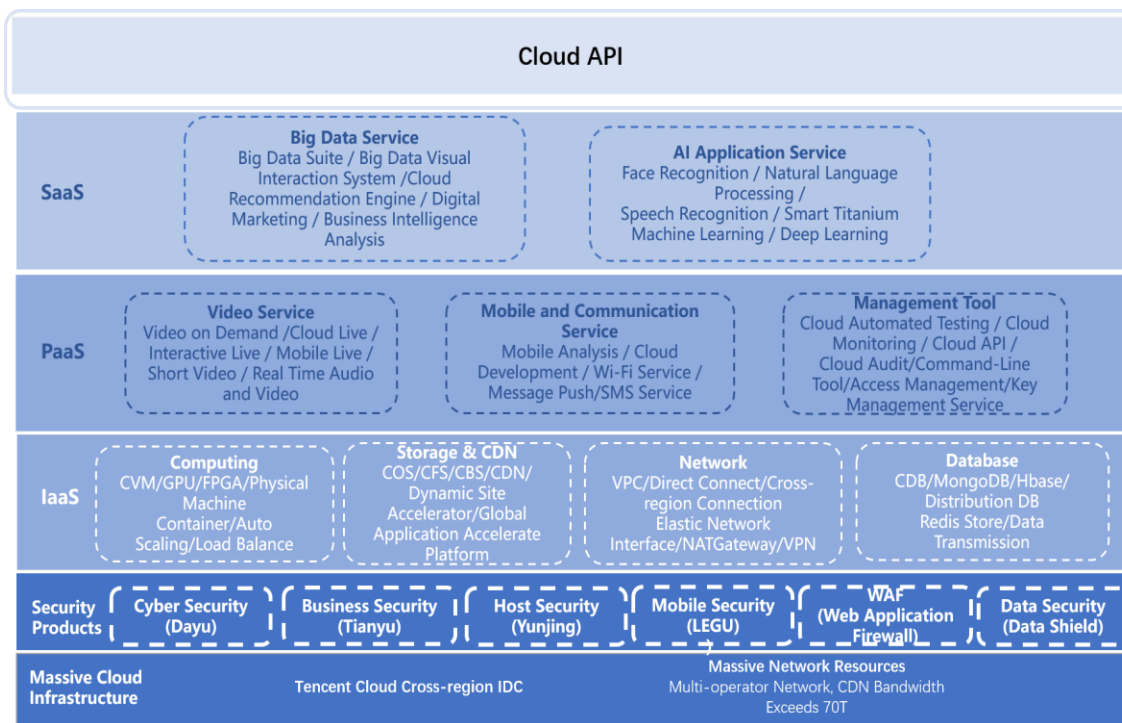


Figure 1 Tencent Cloud Product and Service Structure

Security is essential to Tencent Cloud. Tencent Cloud realized full protection based on comprehensive planning and diversified products and security attributes. Security protection covers the before, during and after event and includes security in physical objects, virtualization, network, host, data, application, business, audit and management. Additionally, Tencent Cloud realized corresponding product security functions, such as authentication, data reliability, and monitoring, and is continuously optimizing product features.

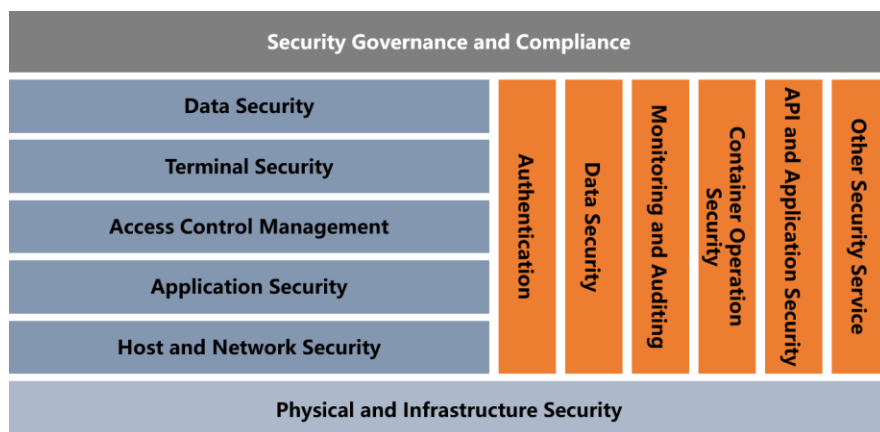


Figure 2 Diagram of Tencent Cloud Security Model

In the following chapters, we will describe how Tencent Cloud can protect you at different security levels. We will cover topics such as infrastructure security (mainly physical security, network security and host security), data security, application and business security (covering application security and business security), operational management security (including security auditing and security management).

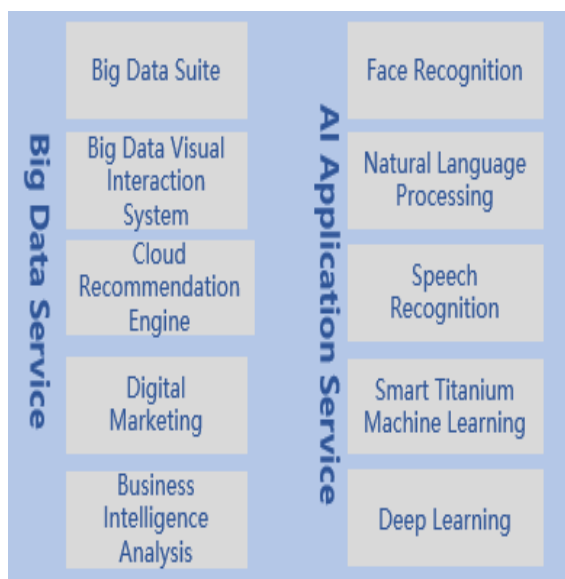
2. Cloud Service Type

Reference and Architecture Model

Tencent Cloud offers you three different types of cloud computing services: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Sometimes it is called SPI¹ models. Now, there are many evolving technologies in building cloud services that make any single reference or architectural model obsolete. One way to look at cloud computing is to think of it as a stack, SaaS is on top of PaaS, and PaaS is on top of IaaS. They are not simple inheritance relationships (SaaS is based on PaaS, and PaaS is based on IaaS), because firstly, SaaS can be based on PaaS or deployed directly on IaaS. Secondly, PaaS can be built on top of IaaS, or it can be built directly on physical resources. As an Internet-based cloud computing service, SaaS, PaaS, and IaaS serve different types of users.

SaaS² (Software as a Service) :

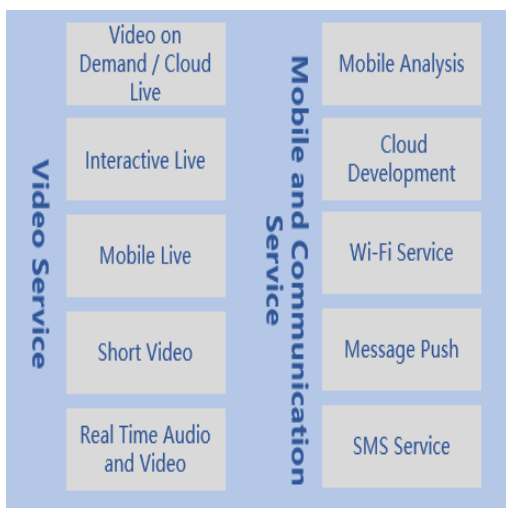
SaaS is an application managed and hosted by Tencent Cloud. You can access it through a client interface on a variety of devices, such as browsers, mobile apps, or light client apps. You don't need to manage or control any cloud computing infrastructure, including networks, servers, operating systems, storages, and more. For face recognition products, you only need to set the product-related properties in Tencent Cloud Console to use the application into your business scenario without managing and controlling any cloud computing infrastructure and application platform environment.



¹ SPI is the three service modes of cloud computing: SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service). The National Institute of Standards and Technology (NIST) defines IaaS, PaaS and SaaS in "The NIST Definition of Cloud Computing" in 2011.

² All definitions are from "CSA Cloud Security Guide V4.0".

PaaS (Platform as a Service) :



Tencent Cloud offers development or application platforms such as databases, application platforms, file storage and collaboration, and even exclusive application processing. You don't need to manage or control the underlying cloud infrastructure such as network, servers, operating systems, or storage. You can control the deployed applications and the configuration of the managed environment on which the application runs. For cloud database type products, you can control the database itself through the Tencent cloud console and cloud API, or you can configure the virtual environment of the subordinate database, but you do not need to manage or control the underlying

infrastructure.

IaaS (Infrastructure as a Service) :



Tencent Cloud provides you with basic computing resources, including CPU, memory, storage, networking and other basic computing resources. You can deploy and run any software, including operating systems and applications. You don't need to manage or control any cloud computing infrastructure, but you can control the choice of operating system, storage space, deployed applications, and control over restricted network components such as routers, firewalls, load balancers, and more. Typical products such as cloud server CVM.

SecaaS (Security as a Service) :



Tencent Cloud provides security capabilities as a cloud service. This includes specialized security-as-a-service offerings and security features built into general-purpose cloud computing products. SecaaS covers a wide range of possible technologies. These services (usually SaaS or PaaS services) are often not just used to protect cloud deployments; they are equally likely to help protect traditional on-premise infrastructure.

For example, Data Shield provides you with comprehensive protection across SaaS, PaaS, and IaaS.

3. The Security Responsibility Sharing Model

What level of security can Tencent Cloud provide?

What other aspects of security control do I need to consider?

Utilizing a unified underlying architecture and resource sharing approach, Tencent Cloud is committed to providing customers with networking, storage and computing and other recourse they need. Currently, more and more customers consider cloud computing security as one of the metrics when selecting a cloud computing provider, cloud products and services. Adhering to the open and shared nature of cloud computing services, Tencent Cloud continues to enhance its cloud computing security services capabilities and work with customers to build better security systems for cloud services and data. It is precisely because of these cloud computing features that Tencent Cloud will introduce the three cloud computing architecture products and services currently available in this chapter, from the perspective of business operations, to introduce the information security responsibility between you and Tencent Cloud. In Chapter 6, you can learn more about Tencent Cloud's protection capabilities at the data security level and the security practices you can implement as data owners.

Based on information assets and product functions, Tencent Cloud has established the following information security responsibility sharing model. The light blue part is defined by Tencent Cloud, the light gray part is defined by customers, and the grey white part indicates that Tencent Cloud and customers will share the corresponding responsibility:

	IaaS	PaaS	SaaS	
Customer Responsibilities	Data Security	Data Security	Data Security	Shared Responsibilities
	Terminal Security	Terminal Security	Terminal Security	
	Access Control Management	Access Control Management	Access Control Management	
	Application Security	Application Security	Application Security	Tencent Cloud Responsibilities
	Host and Network Security	Host and Network Security	Host and Network Security	
	Physical and Infrastructure Security	Physical and Infrastructure Security	Physical and Infrastructure Security	

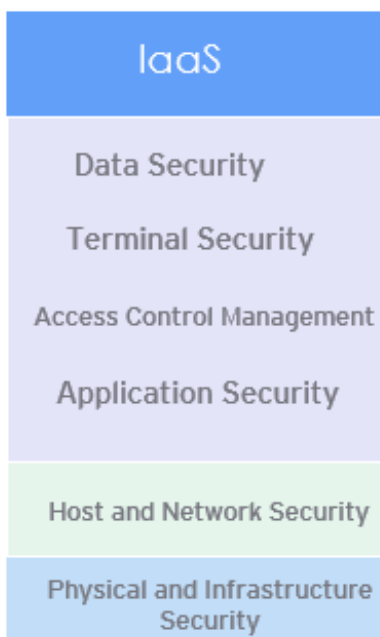
Figure 4 Tencent Cloud Information Security Responsibility Sharing Model

Tencent Cloud explains the different security attributes in the above figure as follows:

- **Data security:** Security management of the customer's business data in the cloud computing environment, including collection and identification, classification, permissions and encryption;

- **Terminal security:** Security management of service-related operating terminals or mobile terminals, including hardware, systems, applications, permissions, and data processing-related security controls;
- **Access control management:** Access rights management for resources and data, including user management, rights management, authentication, etc.;
- **Application security:** Security management of business-related applications in the cloud computing environment, including the design, development, release, configuration and use of applications;
- **Host and network security:** Host and network security management in a cloud computing environment, where the host level includes the underlying management of cloud products such as cloud computing, cloud storage, cloud databases (such as virtualization control layer, database management system, and disk array network) and use management (such as virtual host, image, CDN, file system, etc.); network level includes virtual network, load balancing, security gateway, VPN, leased line, etc.;
- **Physical and infrastructure security:** Data center management, physical facility management, and physical server and network device management in the cloud computing environment.

In this chapter, Tencent Cloud is going to introduce you to the responsibility sharing model based on different SPI cloud computing service types:



IaaS structure model:

Tencent Cloud provides customers with basic cloud products, including cloud server CVM, load balancing, Blackstone physical server, CDN, etc. Tencent Cloud is responsible for the physical and infrastructure security of the entire cloud computing environment; customers using Tencent Cloud are responsible for data security, endpoint security, access control management and application security.

Customers and Tencent Cloud are responsible for the security management at host and network level. At such level, Tencent Cloud provides security management measures including vulnerability discovery, patch repair, upgrade and update, and audit monitoring. Customers are required to securely control the operating system of the purchased cloud host, network communication between cloud hosts, and network communication inside out.

Furthermore, Tencent Cloud provides basic external DDoS protection capabilities to protect all types of resources in the cloud computing platform network from denial of service attacks from the Internet; customers are also required to maintain and manage the purchased cloud products and internal data, cases such as a cloud host actively or passively launches a malicious attack (such as DDoS attack, network sniffing, virus Trojan attack, etc.) due to improper customer management are not within the scope of Tencent Cloud's responsibility.

Taking the cloud server CVM as an example, users do not need to worry about the security responsibilities related to infrastructure (such as physical and infrastructure) when using the cloud server CVM. Users need to update the host operating system using the cloud server CVM in a timely manner, and at the same time, provide sufficient security control for network communication between CVM and internal and external network access. At the same time, users need to ensure the security of their own data stored in the cloud database CVM, guarantee the security of the terminal using CVM, do a good job of access control strategy and management, and be responsible for application security on CVM.

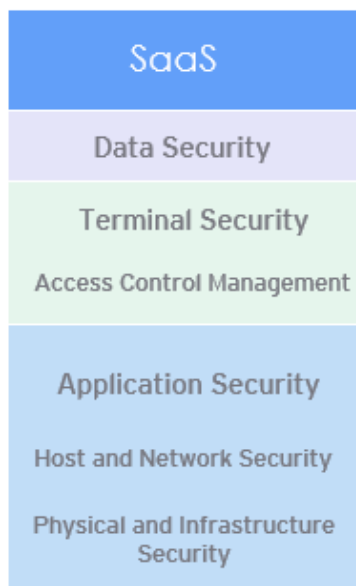
PaaS Structure model:

Tencent Cloud provides customers with platform-based cloud products, which includes cloud databases, cloud caches. Tencent Cloud is responsible for the physical and infrastructure security of the underlying cloud computing environment, as well as the host and network layer security that provides support for platform-like cloud products. Customers are responsible for the data and endpoint security from using such products and services from Tencent Cloud.

Application security and access control management are shared between the customer and Tencent Cloud. In terms of application security, Tencent Cloud reduces the cost and investment of information security of customers by developing and implementing detailed security control measures for platform-based cloud products; customers are responsible for the proper configuration of platform-based cloud products and the integration of additional security capabilities (such as identity management) based on security needs. Furthermore, in terms of access control management, Tencent Cloud can provide role-based access control, account protection, multi-factor authentication, single sign-on and other security capabilities on demand through the console. On the other hand, customers should manage and set up accounts and permissions of cloud products based on business needs and compliance requirements.

Taking a cloud database as an example, users do not need to worry about security requirements at the infrastructure level, host level, and network level when using cloud database products. Users need to configure the platform products through the Tencent cloud official website console or cloud API to ensure the security of the platform products at the application level. At the same time, they should manage and allocate the account and permissions of the platform products to ensure the security of access control.





SaaS Structure Model:

Tencent Cloud provides customers with application cloud products, including cloud communication, cloud search, and Youtu face recognition. Tencent Cloud is responsible for security from the underlying physical and infrastructure, to the host and network level, as well as the application level; customers are responsible for data security.

Access control management and terminal security are shared by the customer and Tencent Cloud. Similar to the security responsibility of the PaaS structure model, in terms of access control management level, Tencent Cloud is responsible for providing role-based access control, account protection, multi-factor authentication, single sign-on and other security capabilities for customers on demand. On the other hand, customers should manage and set up account and permission of cloud products based on

business needs and compliance requirements, so as to ensure they are used in a safe and controllable environment. In terms of terminal level, Tencent Cloud can provide customers with terminal security protection capabilities such as terminal device type identification, login protection, application security evaluation and reinforcement, application distribution channel monitoring, security SDK, and real machine adaptation detection. Meanwhile, customers are responsible for the use restrictions and access control of terminal devices (such as laptops, PC terminals, mobile phones, etc.), as well as the usage of terminal security capabilities provided by Tencent Cloud to obtain perfect security protection.

In the entire SPI Cloud computing structure:

For IaaS, the architecture, servers, network hardware, and virtualization should be managed by the platform vendor. Customers have or share responsibility for the protection and management of operating systems, network configurations, applications, identities, clients and data.

For PaaS that is built on IaaS deployments, vendors have responsibility for the management and protection of network controls. Customers has responsibility or shared responsibility for the protection and management of applications, identities, clients and data.

For SaaS, the application is provided by the corresponding vendor, and the client is isolated from the underlying components. Despite this, customers are still responsible for ensuring that data is properly categorized and sharing responsibility for managing their own users and end devices.

4. Risk and Compliance

Your business will be more efficient when you choose to build services on cloud, but at the same time you will have to deal with data security and compliance. We protect your cloud security and understand your compliance considerations.

We have always been committed to improving the cloud security system, building security compliance, and creating cloud security standards as well as big data security standards since day one. Moreover, the cloud security environment created by Tencent Cloud has entered a new stage after advancement at different aspects.

4.1 Industry Cloud Certification System

4.1.1 Cloud System Certification



CSA STAR Cloud Security Certification

The STAR Cloud Security Assessment is an international certification for cloud security features launched by the internationally leading non-profit Cloud Security Alliance. It expands the ISO/IEC 27001 information security management system and combines the Cloud Security Matrix (CCM) to visualize the unique issues of cloud security, providing users with an intuitive overview of security architecture assessment.



Trusted Cloud Service Certification

Trusted Cloud Service (TRUCS) certification is a data center alliance organization composed of more than 100 industry members in China. It is tested and evaluated by China Information and Communication Research Institute (Telecommunication Research Institute of Ministry of Industry and Information Technology). The evaluation of multi-dimensional and transparent security indicator data provides an important and transparent reference for users to choose secure and trusted cloud services. Among them, “Cloud Service User Data Protection Capability” is an important basis for cloud providers to provide protection for customers on the cloud data. Tencent Cloud Public Cloud Platform, Financial Cloud Platform and Private Cloud are all assessed by cloud service user data protection capabilities.

This standard proposes a cloud computing user data protection reference framework from the perspective of users, and is divided into two levels: basic level and enhanced level according to the corresponding technical requirements. On the one hand, it provides guidance for cloud computing enterprises to establish a standardized user data protection system and guarantee user data security. On the other hand, it provides a basis for third-party organizations to evaluate the user data security protection capability of cloud computing service providers. It also provides a reference for users to choose cloud computing services with well-protected data. Data is well protected by cloud computing services. Data security requirements in the “Cloud Computing Service Protocol Reference

Framework” include data persistence, data destructibility, data portability, data privacy, data right to know, and service auditability. The cloud service data protection capability grading reference framework comprehensively covers three stages of data security pre-prevention, in-process protection and post-tracking, enabling cloud computing service providers to achieve an overall improvement in the “security” protection of data based on “trustworthy” data.

Tencent Cloud’s object storage service, data center VPN service, local load balancing service, gold medal operation and maintenance special assessment, cloud database service, cloud cache service, cloud hosting service, etc. all passed the trusted cloud service certification. To meet the service level agreement (Service Level Agreement, SLA), Tencent effectively endorsed the data storage persistence, data privacy, fault recovery capability, service availability and other indicators.



Big Data Product Capability Certification

Big Data Product Capability Certification is a special certification and industry standard that is led by the Data Center Alliance for the basic capabilities and performance of big data products. The certification covers seven dimensions: function, operation and maintenance capability, multi-tenancy, availability, security, scalability, and compatibility. There are 38 indicators in total, including data review, technical testing, vendor mutual evaluation, and expert review. The certificate aim to assist users in comprehensively examining the functions and features of big data products.

Tencent Cloud’s big data products took the lead in passing the big data product capability certification in 2016, becoming the first large-scale Internet company in the enterprises that passed the industry standard certification, and proved its ability to accumulate data mining and machine learning engine performance.



Information security level protection certification

Information security level protection is a basic system for information security assurance in China, and it is the fundamental guarantee for protecting information development and safeguarding national information security. The level of security protection of information systems is based on the importance of information systems in national security, economic construction, social life, as well as factors such as the damage to national security, social order, public interests, and the legitimate rights and interests of citizens, legal persons, and other organizations if it is attacked. The level of security protection of information systems is divided into five levels, where the fifth level is the highest system level.

According to the “Administrative Measures for the Protection of Information Security Levels”, and related regulations, Tencent Financial Cloud Platform passed the four-level filing and evaluation. Tencent public cloud platform, Tencent cloud platform customer service system, Tencent cloud platform billing system, Tencent cloud platform operation and maintenance management system passed three-level evaluation.



The Motion Picture Association of America (MPAA)

The Motion Picture Association of America (MPAA) has established a set of best practice standards for securely storing, processing, and delivering protected media content. MPAA best practices are designed to familiarize application and cloud service providers who are working with MPAA members on content security requirements. Media companies can use these best practices to conduct risk assessments and security audits of content management. Tencent Cloud has adopted a self-assessment approach to ensure that its management of customer content complies with the Motion Picture Association of America (MPAA) Content Security Model Guide.

The components of the MPAA Movie Content Security Template are based on the relevant ISO standards (27001-27002), security standards (i.e. NIST, CSA, ISACA and SANS) and industry best practices. ISO 27001, ISO 27017, ISO 27018, PCI DSS, and CSA STAR are important compliance programs of Tencent Cloud and have passed third-party audit certification.

4.1.2 ISO/IEC Series Certification



ISO/IEC 22301:2012 Certification

ISO/IEC 22301 is the first international standard focusing on Business Continuity Management (BCM), which provides a complete and versatile BCM methodology that enables companies to achieve internationally recognized best practices. This certification applies to large, medium and small public and private organizations in all industries, and is particularly suitable for industries in high-risk and highly regulated environments, such as finance, IT communications, manufacturing, etc. In the operation process of the enterprise business, the process is often affected by various internal or external factors. In severe cases, it may even cause the business to be interrupted, and the unexpected interruption will bring significant losses to the enterprise. In order to reduce risks, business continuity management has received more and more attention.

Tencent Cloud is one of the first cloud service providers in China to pass the on-site audit of this certification. By establishing a formal business continuity management process, it ensures the continuity and stability of its business. At the same time, Tencent Cloud provides you a framework with organizational flexibility and effective response capability, builds up an overall management process framework with resilience to protect your business from interruption, and maintains your interests, reputation, brand and value creation activities.



ISO/IEC 27001:2013 Certification

ISO/IEC 27001: 2013 Information Security Management System is the most authoritative, rigorous and most widely accepted and applied system certification standard for information security in the world. Obtaining this certification means that the company has established a scientific and effective information security management system to unify the pace of enterprise development strategy and information security management, and has ensured that the corresponding information security risks are properly controlled and properly addressed.

Tencent Cloud is the first cloud service provider in China with ISO/IEC 27001:2013 certification. Through customized information security management control measures and institutional framework for protecting information assets, and the following on PDCA's continuous improvement route, Tencent Cloud commit to your information security to provide reliable information services and related security protection.



ISO/IEC 20000-1:2018 Certification

ISO/IEC 20000-1: 2018 is a set of international standards for IT service management. The system regulates the management of information technology services of enterprises, from the establishment, implementation, operation, monitoring, review, maintenance to improvement models. It assists enterprises to continuously identify and manage related information technology issues, strengthen communication with users, and establish a set of self-improving standardized service system.

Tencent Cloud is certified to ISO/IEC 20000-1: 2018, the scope of certification includes cloud computing services, managed services and disaster recovery services. Tencent Cloud strictly adheres to the service-oriented attitude and improves the mechanism of information technology service and communication between you and the cloud.



ISO/IEC 9001: 2015 Certification

ISO/IEC 9001: 2015 is by far the most mature quality management system in the world. The system provides guidance programs and norms around enterprise products or services, and promotes the product quality management framework for enterprise products or services. It is the foundation for enterprise development and growth.

Tencent Cloud is the first company in China certified ISO/IEC 9001:2015 CNAS (China National Accreditation Service for Conformity Assessment) and ANAB (National Accreditation Board for Accreditation of the US) in the field of cloud computing. The scope of certification covers cloud computing services, hosting services and disaster recovery services, etc.



ISO/IEC 27017:2015 Certification

ISO/IEC 27017:2015 is an international standard that complements ISO/IEC 27002:2013 and enhances the control of threats and risks in cloud computing vulnerabilities. This certification provides 37 ISO/IEC 27002 guidance and 7 control schemes not available in ISO/IEC 27002. Both cloud service providers and cloud service customers can use this guidance to effectively design and implement cloud computing information security controls.

Tencent Cloud's ISO 27017 guidance certificate not only demonstrates that we will always adopt internationally recognized best practices, but also demonstrates that Tencent Cloud has a high-precision control system dedicated to cloud services.

4.1.3 Privacy Certification



ISO/IEC 27018:2014 Certification

ISO27018 is an international standard protocol promulgated by the International Organization for Standardization (ISO) in 2014 and is the first international code of conduct focused on the protection of personal information in the cloud. ISO27018 certification demonstrates that companies have achieved high standards of industry best practices in protecting enterprise data, intellectual property, documentation, and cloud IT system security.

Tencent Cloud's personal information protection management system has entered the global advanced ranking of cloud service providers, providing Tencent Cloud customers with a solid foundation of trust and solid cloud security.



Cloud Infrastructure Services Providers in Europe (CISPE)

CISPE, the European Cloud Computing Leadership Alliance, is committed to serving millions of customers in Europe. Its Personal Data Protection Code of Conduct follows the recently implemented GDPR to ensure that cloud-compliant providers that comply with the Code of Conduct do not access or use customer data for their own purposes and increase the compliance of cloud service providers with GDPR requirements.

This certification is not only the proof of Tencent's comprehensive strength, but also shows that Tencent Cloud has become an excellent choice for data business compliance of companies that develop overseas markets.

4.2 Security compliance

With the continuous evolution of cloud computing technology and security technology, as well as the increasingly complex regulatory requirements of the industry, security compliance has become a major challenge for cloud service providers. Tencent Cloud is committed to establishing an efficient internal control system, closely following the compliance requirements of different industries, fields and countries, and improving compliance in terms of institutional processes and control activities.

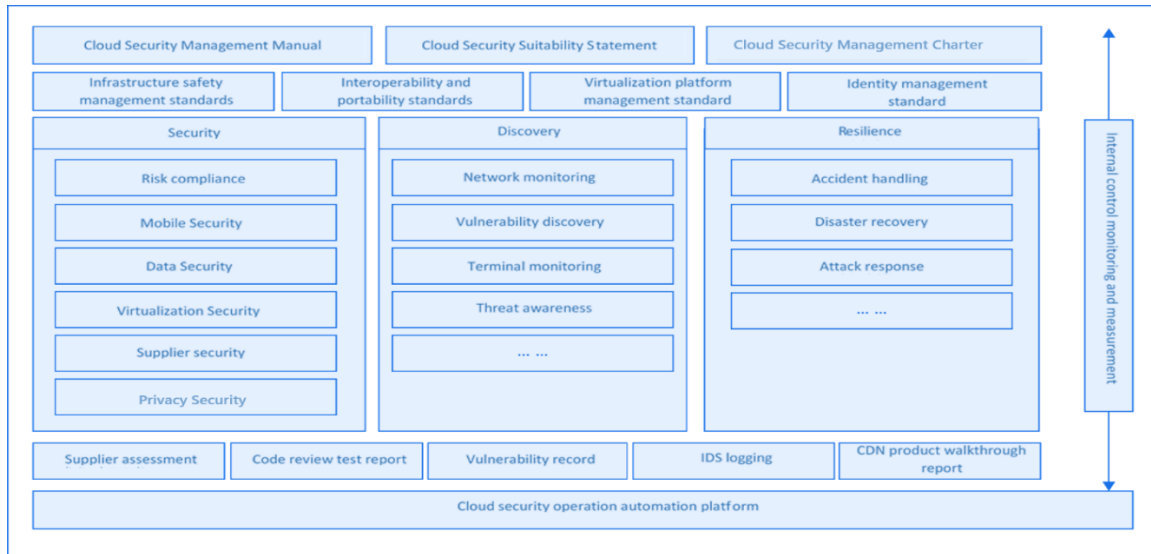


Figure 5 Tencent Cloud Security Internal Control System

Tencent Cloud built an integrated cloud security internal control system guided by the cloud security management charter and cloud security management manual. We created corresponding compliance standards for aspects such as infrastructure security management, interoperability and portability, virtualization platform management, and identity authentication management with detailed compliance requirements of security, discovery and resilience. We ensure the efficiency of our internal security control system via internal monitoring and measurement.

At the same time, we have been improving our security compliance practices. We figured out how to build our security compliance system, developed the whole internal process, and adapt to global regulatory requirements quickly. Tencent Cloud keep establishing and implementing a cloud security compliance system continuously.

4.2.1 Identify External Compliance Requirements and Security Threats

Tencent cloud is a global service and has to comply with both domestic and international requirements and identify different security threats. We adapt to domestic and international compliance requirements and identifies security threats to ensure security compliance.

4.2.2 Adopting Advanced International and Industry Standards

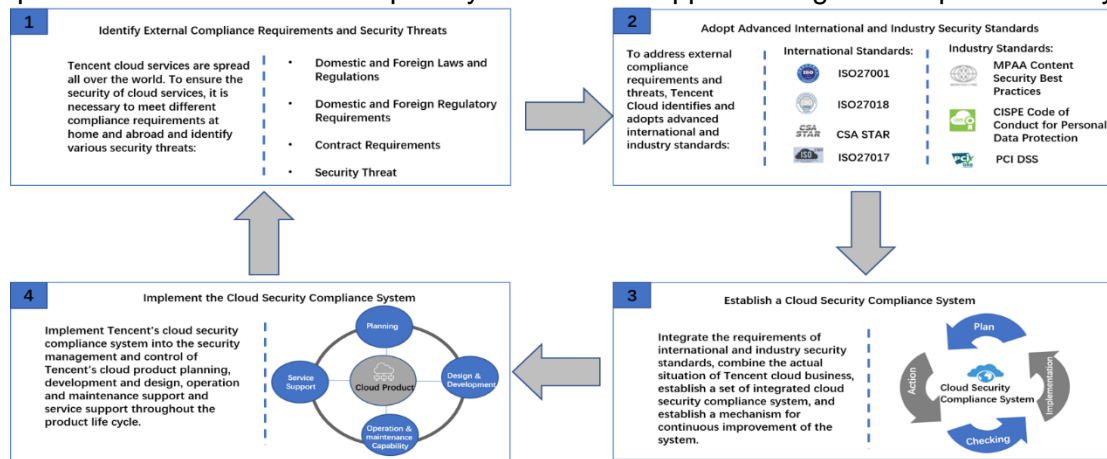
In response to external compliance requirements and threats, Tencent Cloud identifies and adopts international and industry security standards.

4.2.3 Establish a Cloud Security Compliance System

Tencent Cloud integrates the requirements of international and industry security standards, combines the actual situation of Tencent cloud business, establishes a set of integrated cloud security compliance system, and establishes a mechanism for continuous improvement of the system

4.2.4 Cloud Security Compliance System Implementation

Tencent Cloud implements Tencent's cloud security compliance system into the security management and control of Tencent's cloud product planning, development and design, operation and maintenance capability and service support throughout the product life cycle.



4.3 Security Compliance Service

Our experienced industry experts provide secure, reliable and professional security compliance products and services.

4.3.1 Cybersecurity Classified Protection Compliance Service

Tencent Cloud Cyber Security Classified Protection Compliance Service, associated with the local classified protection assessment center, provide localized, systematic and professional classified protection security assessment services. Additionally, Tencent Cloud provides a complete security cooperation environment with complete security products and services to help you assess and improve classified protection mechanism. You can submit your application online, accept the assessment institution recommended by Tencent Cloud, and place an order in the cloud market to start the one-stop evaluation process.

4.3.2 PCI-DSS Compliance Service

Tencent Cloud PCI-DSS Compliance Services works with third-party assessment agencies and consulting organizations to provide professional, systematic and customized PCI-DSS compliance services. Additionally, Tencent Cloud provides a complete security cooperation environment to provide complete security products and services to help you evaluate and rectify, improve security capabilities, and quickly pass PCI-DSS assessments. You only need to submit your application online, accept the third-party

evaluation or consulting agencies recommended by Tencent Cloud, and place an order in the cloud market to start the service process in one stop.

4.4 Privacy Protection

We think user need is our first priority, and focus on building long-term customer relationships based on trust. We protect customer account information and hosted customer content through advanced technologies and comprehensive operation and management.

In order to better provide customers with safe and reliable cloud products and services, Tencent Cloud will collect your personal or corporate information upon your account registration, management, or real-name authentication, and strictly follow the [Privacy Policy](#)¹ and [Data Privacy and Security Agreement](#) for collection, usage, storage and sharing of personal data.

Tencent Cloud will not attempt to access or disclose your customer content. To ensure that you have exclusive ownership and control over your customer content, Tencent Cloud will endeavor to inform you about the privacy protection and data security technologies and management measures that have been implemented.

Here, we once again declare that Tencent Cloud is committed to protecting the information of customers around the world and complying with applicable privacy laws in the countries or regions in which the business market is located.

Tencent Cloud passed the CISPE (Cloud Infrastructure Services Providers in Europe) Personal Data Protection Code of Conduct certification, becoming the first cloud service provider in China to receive this certification. CISPE is currently the only non-profit organization in the European Union that provides data protection codes of conduct for cloud service providers. The Code of Conduct is based on the compliance requirements of GDPR. This certification is not only the embodiment of Tencent's comprehensive strength, but also shows that Tencent Cloud has become an excellent choice for data business compliance of companies that enter overseas markets

For more information on CISPE please visit:
<https://cloud.tencent.com/document/product/363/20373>

¹ Privacy Policy and other Terms and Policies can be referenced at:
<https://intl.cloud.tencent.com/document/product/301>

5. IT Infrastructure Security

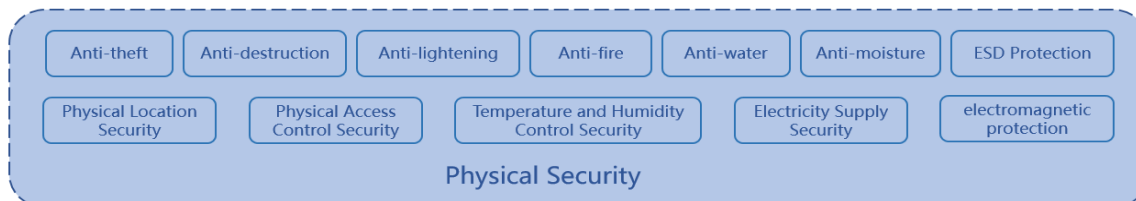
Can other accounts access my Cloud environment?

How does Tencent Cloud guarantee products and services can be continuous and highly available?

What types of security products and services does Tencent Cloud offer?

5.1 Physical Security

As a cloud computing service provider, Tencent Cloud focuses on providing each customer with a safe, stable, sustainable and reliable physical network infrastructure. Following international standards and regulatory requirements related to data center, Tencent Cloud has established a comprehensive security management program from policy to process management, and to ensure the physical and environment security of cloud computing data centers with strict monitoring and auditing, as well as through continuous improvement.



5.1.1 IT Infrastructure Security

Infrastructure security such as electricity, air conditioning, fire protection and ESD protection is the most basic environmental facility for cloud computing data centers, and one of the most important aspects to ensure availability. Each Tencent Cloud data center in the world is chosen, constructed or leased in accordance with relevant international standards and local security requirements. Each data center power system and air conditioning system uses a high-stability, fully redundant system that ensures power and cooling continuity in the data center in the event of any single point of failure; each data center is equipped with a complete fire protection system, including fixed area fire detection system, automatic gas fire extinguishing system, and manual fire extinguishing device for emergency use; all data centers are equipped with anti-static floor, and grounding wires are installed in cabinet, cable trough, etc., to prevent static electricity from causing damage to the equipment. Additionally, Tencent Cloud also requires all data center personnel to regularly receive business continuity drill training to ensure the implementation of data center infrastructure security is effective.

The computer clusters of Tencent Cloud are distributed in multiple locations around the world, which are composed of “regions” and “available zones”. Each region is an independent geographic region. Each region has multiple isolated locations, known as zones. Region and available zone can most directly represent the coverage area of the computer room. **Region:** Tencent cloud is completely isolated between different regions to ensure the maximum stability and fault tolerance between different regions. Currently, it covers South China, East China and North China, and has nodes in Hong Kong and Singapore for Southeast Asia, Frankfurt node for Europe, Silicon Valley node for North America and Toronto node for Canada. We will gradually increase the regional supply to increase the coverage of nodes. It is recommended that you choose the region closest to your customers to reduce the access delay and improve the download speed. The behavior of users to initiate instances, view instances and so on are distinguished by region. **Available zone:** Available zone refers to the physical data center of Tencent Cloud and the power and network of data centers are independent in the same region. The objective is to ensure that the breakdowns in available zones are isolated from each other

(except for large disasters or large power failures), and to ensure that there is no further influence due to the breakdown, so that the online services of user's business can continue. By initiating instances in a separate available zone, the user can protect the application from a single location failure. When the user starts the instance, he can select any available zone under the specified region.

Customers can deploy data and systems in different regions or available zones according to their business development needs and data security requirements to ensure the disaster-tolerant requirements of the service. At the same time, Once the customer chooses Tencent Cloud, they can get the IT infrastructure and high-availability features of the Tencent Cloud data centers such as power supply systems, air conditioning systems, fire detection and protection systems, and power systems with disaster recovery and redundancy capabilities.

5.1.2 Access Control Policy

Tencent Cloud has classified different areas of the data centers into four security levels:

- **Level 4 security area:** A public area that does not store equipment and does not affect the operation of the equipment room, such as the office parks park.
- **Level 3 security area:** Area that stores documents with business information, office areas with business information, such as office room, operation centers, etc.
- **Level 2 security area:** Area that stores non-production equipment and does not directly affect the operation area of the equipment room, such as warehouses.
- **Level 1 security area:** Area that stores the operational equipment and affects the overall operation area of the equipment room, such as the customer's exclusive computer room and infrastructure area.

Each data center has strict infrastructure and environment access controls based on different levels of regional security requirements. According to the data center personnel category and access rights, a complete personnel access control matrix is established in the access control authorization system to effectively control the access and operation behavior of various personnel in the data center. For internal or external employees, the accuracy of the authorization is checked regularly. When an employee resigns, all his/her permissions will be revoked and access control items such as access cards should be returned. For visitors, they must provide a valid ID number, access reason, access time, access area and other information in advance to apply for authorization. After getting the approval, the designated area of the data center can be accessed at the agreed time, and the visitor should be accompanied by a dedicated person during the whole visit.

All types of visits or access of staff to the data center are subject to identity check and personal belongings inspection, and carried items should be registered. From the perspective of environment control, each data center also has strict management regulations and control measures for vehicle access. Information of all employees' personal vehicles, supplier trucks, etc. need to be registered, and only allow authorized vehicles to enter the peripheral environment of the data center. Public transport such as taxis is prohibited from entering the data center park in principle.

The monitoring and management of the Tencent Cloud data centers cover the equipment room, the work handover area, the entrances and exits of each building in the park and of

the park itself. They are equipped with 24/7 video surveillance alarm systems that are without blind spots (all monitoring records have adequate retention period and secure storage), and are guarded by the security room 24/7. Tencent Cloud also requires all data center operators and builders to have the corresponding work qualifications and experience, and conducts regular security awareness and ability training for relevant personnel.

5.1.3 Security Assessment and Audit

Security Inspection Management

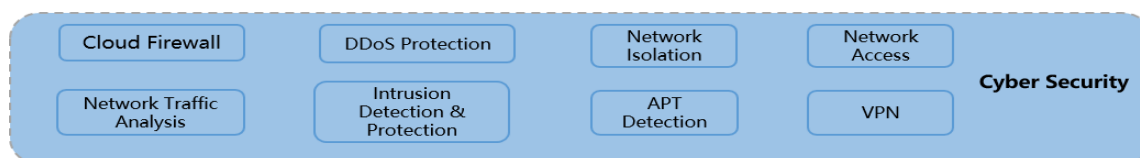
The security personnel of each Tencent Cloud data center strictly follow the inspection list and inspection plan when conducting inspections on the data center equipment rooms and equipment. The frequency of each inspection is no less than 12 times per 24 hours and covers the entrances and exits of the building, surrounding of the building and the inside of the building. The inspection time are recorded and signed at each point of inspection. If a security violation is discovered, the data center equipment room management emergency procedures will be executed immediately.

Security Incident Management

Each data center has developed a physical security contingency plan, and data center staff undergo regular security practices. In the event of a physical security incident, the plan will be acted upon immediately for the relevant personnel to protect the client's assets to the greatest extent possible. All security incidents are documented and analyzed in detail for continuous improvement and enhancement of existing security management practices and policy.

5.2 Network Security

Tencent Cloud provides a mature network security architecture, including multiple protection mechanisms such as firewall and web application protection to cope with various threats from the Internet.



5.2.1 Network Communication Security

Clients communicating via Tencent Cloud platform are protected by the encryption of the HTTPS security protocol. Users can also choose the secure channel provided by Tencent Cloud for network data transmission, such as the virtual private network VPC between the internal instances of the cloud computing platform, and the private line network connecting the cloud computing platform through the Internet and VPN.

Additionally, the Cloud API interface provided by Tencent Cloud's product has security capabilities such as HTTPS encryption, signature verification, and status monitoring, which can provide port-level communication security for your business.

5.2.2 Network Isolation

Tencent Cloud implements strict internal network isolation rules, through physical and logical isolation of the internal office network, development network, test network, production networks' access control and border protection; Tencent Cloud ensures that unauthorized personnel are prohibited from accessing any internal network resources. Also, all employees who need to go from the company network to the production network for daily operation and maintenance must log in to the production system through the bastion hosts.

At the same time, Tencent Cloud employs virtualization control, internal private network isolation, web console rights allocation and authentication, session ID and access key security for its users, which can ensure each user only access resources that he/she has purchased, and effectively achieve isolation between multiple users.

5.2.3 Network Redundancy

Tencent data centers are located worldwide, covering China, United States, South America, Europe, Asia Pacific and other areas. Each network is connected to multiple operators in multiple regions, building its disaster recovery capability of Tencent Cloud across regions. Effectively reducing the impact of an operator's public network failure. The plan will also launch multiple regions and availability zones in succession, providing more enterprises and entrepreneurs with a global cloud service experience integrating cloud computing, cloud data and cloud operations.

The Tencent Cloud infrastructure adopts the N*N construction methods where it cooperates with route-level path priority and route reachability traffic engineering scheduling to ensure that network services are not interrupted due to a single device fault. Tencent Cloud computing nodes are also N*N construction methods. A single computing node automatically cancels in real time through a scheduler when a fault occurs, effectively ensuring the availability of user services.



Figure 6 Schematic Diagram of Tencent Cloud Global Network

5.2.4 Attack Protection

For DDoS attacks, Tencent Cloud provides you with effective protection. Among them, DDoS protection (Named as Dayu), access to 30-line BGP lines, comprehensive coverage of domestic mainstream and small and medium-sized operators, bringing a speed, stable access experience, while having 5T or more of protection bandwidth, is the largest BGP high-defense product in China. It can provide stable protection for all kinds of customers such as games, finance, government, etc. By October 2018, Tencent Cloud has defense nearly 250,000 DDoS attacks this year, with a peak of more than 1200Gbps.



Figure 7 January –September 2018 Tencent Cloud DDoS Attack – Defense Statistics

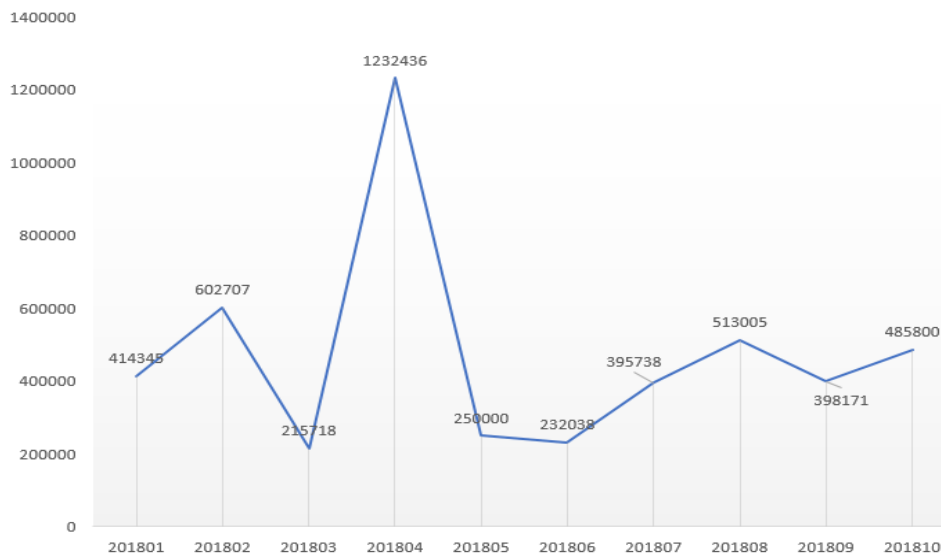


Figure 8 January –October 2018 Tencent Cloud DDoS Attack – Defense Traffic (Mbps) Statistics

5.3 Customer-oriented Basic Cloud Products

5.3.1 Security Products

I. Dayu Network Security

Tencent Cloud DDoS Protection (Dayu) is a protection solution launched by Tencent Cloud for the business and brand loss caused by high-traffic DDoS attacks on users such as games, Internet+, finance, and websites. In response to the increasingly serious cyber security challenges and the threat of successive DDoS attacks, Tencent Cloud launched the global integrated DDoS protection system of Dayu GDS (Global Defense System): overall planning and design prior to the event, providing strong protection capability in the event, and traceability after the event. According to the Internet business needs of different customers, Dayu Network Security provides diversified protection solutions:

- **Basic DDoS protection:** Basic DDoS protection is the free DDoS protection service provided by Tencent Cloud for all cloud CVM, LB and other devices.
- **BGP High Defense:** BGP high Defense can easily and effectively cope with DDoS and CC attacks to ensure stable and normal business. The main advantage of BGP high-defense package is that it can directly load defense capabilities onto cloud products.
- **BGP High Defense IP:** BGP High Defense IP ensures that the protected user can still provide external service services while the attack is on.
- **DNS High Defense:** DNS High Defense has the ability to prevent common network attacks and effectively block large-scale DNS attacks.

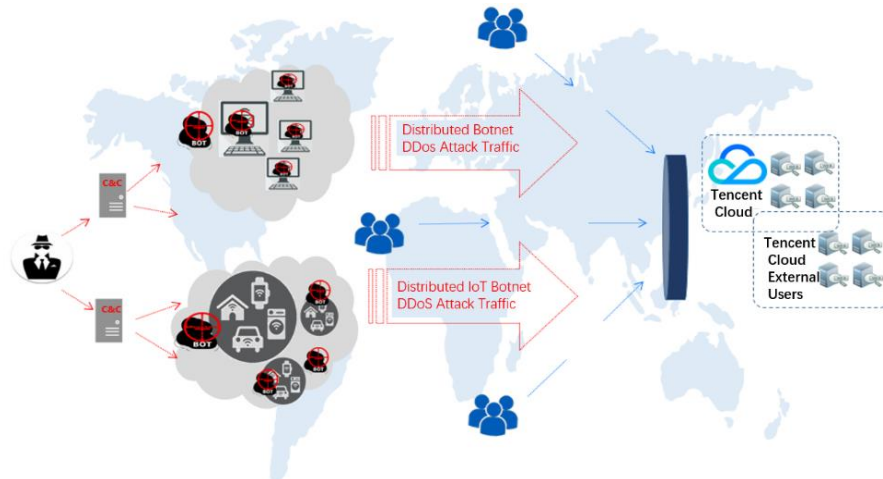


Figure 9 Tencent Cloud Dayu Protection Diagram

II. Web Application Firewall---Web Manager

Tencent Cloud Web Manager is an AI-based one-stop smart protection platform for websites and web services. Traffic accessing the web service site is directed to the Tencent cloud web manager protection cluster, then cloud threat cleaning and filtering are performed before secure traffic is returned to the service site. In this way traffic arriving at the user's business site is secure.

Tencent Cloud Web Manager is the first Web Application Firewall (WAF) in China with machine learning detection technology. AI engine-based WAF advances the web attack detection technology from the regular engine and semantic analysis to machine learning-based web attack detection, which is a turning point of WAF technology, and improves complex and unknown web attacks detection ability. Moreover, AI-based Web attack detection improves self-learning, which helps to enable a self-adapting web attack detection and defense system.

Tencent Cloud Web Manager has comprehensively defended against malicious attacks through Web Intrusion Prevention, 0 Day vulnerability patching, malicious access penalties, cloud backup anti-tampering, Bot behavior management, DNS hijacking detection and other multi-dimensional defense strategies to protect the system and business security operations of the protected website.

- **Web Attack Protection:** Tencent Cloud Web Manager can effectively defend against common web attacks.
- **Vulnerability Virtual Patch:** Tencent Cloud Web Manager actively detects and detects high-risk vulnerabilities in a timely manner and generates protection rules for vulnerabilities.
- **Data Anti-Leakage:** For data theft, Tencent Cloud Web Manager provides before, in and after the event protection strategy.
- **CC Attack Protection:** The website administrator has built-in CC Attack Protection algorithm to block malicious requests, filter garbage access, and effectively defend against CC attacks.
- **BOT Behavior Management:** Tencent Cloud Web Manager classify friendly and malicious BOT crawlers and adopt targeted management strategies.
- **DNS Hijacking Detection:** Web Manager use Tencent to detect probe points and cloud data analysis capabilities to help organizations avoid DNS hijacking problems.
- **Webpage Tampering:** The user's operation synchronizes the update of the website administrator's cache before releasing it, ensuring that the update of the protected webpage is controllable and reliable.

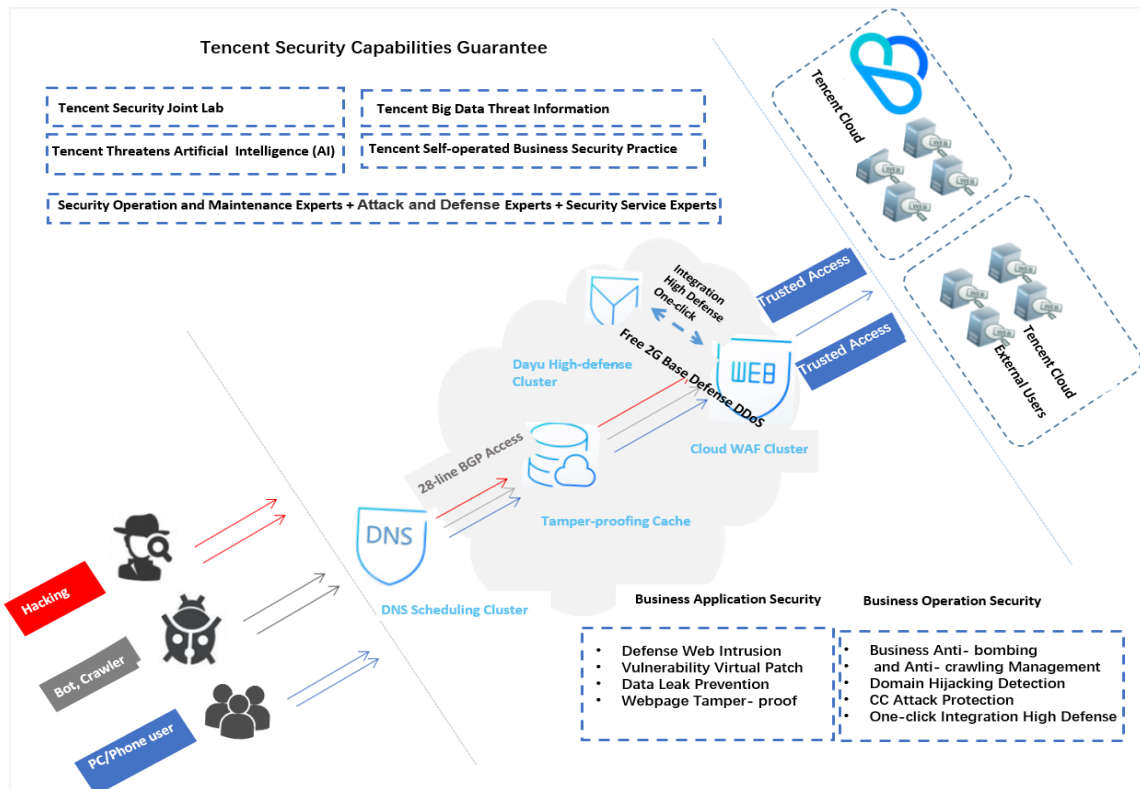


Figure 10 Schematic Diagram of Web Manager

IV. Vulnerability Scanning

Tencent Cloud Web Vulnerability Scanning is a security service for website vulnerabilities detection. Its powerful vulnerability scanning covers large vulnerability database, and its various scanning functions provide 24/7 security detection, security assessment, and security monitoring. It also offers companies repairing suggestions to prevent website security issues and vulnerabilities exploitation. Currently, web vulnerability scanning has been applied and acknowledged in IT, finance, communications, government, energy, military and many other industries.

Tencent Cloud web vulnerability scanning has strong scanning capabilities and various scanning functions. It supports concurrent detection of multiple web applications and periodic normalization detection, and help customers build a strong security risk assessment system.

- **Vulnerability Scanning Service:** The Vulnerability Scanning Service covers a large database of vulnerabilities and supports both generic vulnerability scanning and special vulnerability scanning.
- **Scan Analysis Report:** Tencent Cloud will provide customers with detailed scan reports after conducting vulnerability scanning service.
- **Security Emergency Services:** Vulnerability Scanning has a team of professional security experts who can provide professional security emergency services.

- **Repair Closed-loop Management:** Vulnerability scanning service provides customers with professional repair suggestions, while tracking the repair of vulnerabilities and implementing closed-loop management of the vulnerability lifecycle.

5.3.2 Cloud Computing and Networking

Computing products:

Tencent Cloud Virtual Machine (CVM) is a fast and stable cloud virtual machine. CVM is Tencent Cloud's major product and it provides adjustable computing capacity. Tencent CVM has its unique and innovative features. Efficiency and fast creation: 90% of cloud servers are created within 10 seconds; thousands of cloud servers can be created per minute in a single region. Easy to use & cross available zone hot migration: hot migration of servers is available at different zones in the same region, and service is not interrupted. Reliable and efficient disaster recovery: Tencent Cloud has the unique all-purpose placement cluster, which not only provides multiple availability zones in the same region, but also three-layer disaster recovery across physical machines, racks, and switches in an availability zone. Therefore, it has comprehensive disaster tolerance.

If you have higher demand for resource isolation due to regulatory requirements, Tencent Cloud can provide a dedicated host CDH (CVM Dedicated Host). In addition to the security features provided by the general CVM, CDH can achieve resource isolation at the host level, and the network, memory, and disk are dedicated to tenants. CDH also supports disk degaussing for sensitive business data protection, disk degaussing, and more, to meet your compliance requirements.

Cloud Block Storage (CBS) is a low-latency, high-performance, and highly reliable block storage provided by Tencent Cloud for cloud server CVM. Just like a computer hard drive, you can format, create a file system, etc., for block storage mounted on a CVM instance.

Auto Scaling (AS) automatically adjusts computing resources based on your business needs and policies. The CVM instance can be added or removed just in time according to the timing, period, or monitoring policy, and the configuration can be completed to ensure smooth and healthy operation of the service.

Tencent Cloud provides the following security features in computing relevant products:

- **Image Security:** Image is a copy of the current cloud server instance running environment. It is mainly used to deploy new environments in batches, including the operating system and installed software. Tencent Cloud provides the following two types of images: 1) Public image: provided by Tencent Cloud official, consisting of the basic operating system and the initialization components provided by Tencent, which can be used by all users; 2) Service market image: provided by a third-party service provider. All users can also use the images that have been released to the service market after Tencent Cloud's content review and security verification.
- **Vulnerability Management:** Based on the strong technical support provided by the Tencent United Security Laboratory, Tencent Cloud has built a complete and

- in-depth vulnerability management system covering vulnerabilities discovery, vulnerability handling and vulnerability collection, which conducts comprehensive and in-depth research on vulnerabilities. At the same time, Tencent Security Response Center (TSRC) opened a vulnerability submission platform to all the public to help Tencent improve the discovery and disposal of vulnerabilities.
- **Business Continuity:** To ensure the continuity of customer business, Tencent Cloud has developed a detailed disaster recovery plan for each cloud product (including computing and networking, storage and CDN, cloud database and security cloud products), and regular practices in strict accordance with requirements to ensure the timeliness of disaster recovery plan and feasibility.
 - **Tenant isolation:** Tencent Cloud provides complete tenant virtual resource isolation capability for resources such as cloud server CVM in the virtualization control layer. Different users' network, memory, disk and other resources are controlled by the underlying logic to eliminate the possibility of mutual access.

Network products:

Virtual Private Cloud (VPC) helps you build multiple independent network spaces in the purchased cloud platform resources, and customize network segmentation and IP addresses, custom routing policies, etc. At the same time, you can deploy Internet-based IPsec VPN tunnel connection to the cloud platform private network with other resources within your enterprise.

Direct Connect (DC) is a highly reliable private network access service provided by Tencent Cloud for enterprise users. You can use dedicated line access to connect Tencent Cloud with your company's network, additional data centers, third-party partners, etc. Connected to achieve a hybrid cloud deployment with high-capacity and high-reliability network interconnection.

Cloud Load Balance (CLB) can help you automatically distribute business traffic from the Internet between multiple CVM instances or other resources in the cloud platform, which enables your business system to achieve a higher level of application response and fault tolerance.

Flow Logs (FL) provides you with full-time, full-flow, non-intrusive traffic collection services. You can store and analyze network traffic in real time to help you solve troubleshooting, architecture optimization, security detection, and compliance auditing and other problems to make your network on the cloud more stable, secure and smarter.

Elastic Network Interface (ENI) is an elastic network interface that binds cloud hosts in a private network and can be freely migrated between multiple cloud hosts. You can bind multiple elastic NICs to the cloud host to implement a highly available network solution. You can also bind multiple intranet IP addresses on the elastic NIC to implement single-host multi-IP deployment.

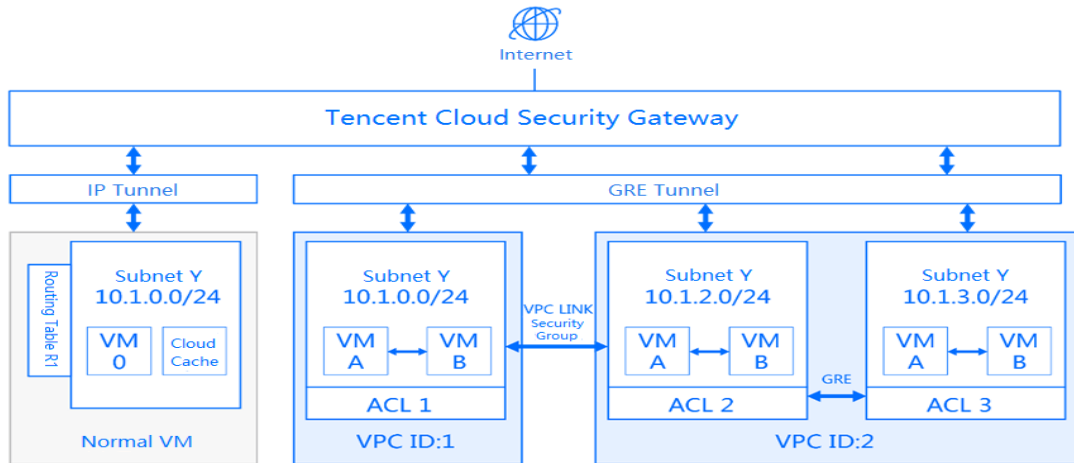


Figure 2 Schematic Diagram of VPC Security Features

For network products, Tencent Cloud implements the following security features:

- **Gateway security:** The NAT gateway is a way for the internal network to access the public network. It can convert the internal network IP address and public IP address of the private network when the internal network is isolated.
- **Network ACLs and security groups:** Network access ACLs and security groups through the private network enable resource access control at the port and instance level to improve network security.
- **Network segregation:** Tencent Cloud implements network isolation through IP tunnel + VPC private network. Each tenant is assigned a different VPCID, ensuring that you can networking freely in the VPC private network without being affected by other tenants.
- **Network Analysis:** By analyzing network traffic within the VPC, you can quickly identify and locate network security threats and improve system security. You can quickly identify high-risk behaviors such as IP scanning, abnormal port access, port rotation access, and security group sniffing, quickly locate high-risk IP and block it through security groups, network ACLs, etc., thereby greatly reducing network security risks.

5.3.3 Storage and CDN

Cloud Object Service (COS) is a highly available, highly stable, and secure cloud storage service for enterprise and individual developers. Any number and form of unstructured data can be placed in the COS, where data management and processing are implemented. COS supports the standard Restful API interface. COS implements the following security features:

- **Anti-theft chain mechanism:** COS provides anti-theft chain configuration function for buckets, which can configure blacklist and whitelist to constrain the access source. It also supports cross-domain access control and strictly manages the source of cross-site access.

- **Multi-regional Storage:** Users can select the nearest storage regions based on the service hotspot and reduce resource acquisition delay. At the same time, support for cross-regional replication and other functions, multi-site copy storage to help customers achieve remote disaster recovery.
- **Perfect privilege system:** Use Tencent Cloud CAM to provide user and resource privilege management mechanism. Operations and resources can be assigned permissions under specified conditions, and the access privilege is managed through ACLs for each resource.
- **Encryption Protection:** HTTPS encrypted connections are supported across the board. For each object, you can choose from a variety of server and client encryption methods including Tencent Cloud KMS service.

Content Delivery Network (CDN), a network-wide content acceleration service, uses the accelerating nodes all over the world to publish business content to the edge nodes closest to users that no need to be forwarded over multiple networks. Avoid forwarding that has high latency, low availability, and other issues due to factors such as geography, bandwidth, and server capabilities such as geographical, bandwidth, and server capabilities.



Figure 3 Schematic Diagram of Tencent Cloud Content Distribution Network Node

At the same time, CDN implements the following functions in access control, security protocols, and network attack protection:

- **Access Control:** By providing filter of requests through the referrer black and white list or IP black and white list settings. Support enhanced URL authentication methods, for example when you need to set access timeliness for a resource, you can use the timestamp anti-theft chain.

- **Security Protocol:** Tencent Cloud CDN supports HTTPS and HTTP2.0 security protocols across the entire network.
- **Multiple attack protection:** CDN-derived SCDN security acceleration service, supports self-written multiple rules for access control, supports WAF protection for return source requests, and has certain DDoS defense capabilities.

5.3.4 Cloud Database (TencentDB)

The cloud database (TencentDB) is the overall brand of Tencent Cloud Database and currently contains all the database services provided by Tencent Cloud.

For example: the relational database CynosDB, MySQL, MariaDB, SQLServer, PostgreSQL, and the distributed database TDSQL, elastic cache Redis, cloud database MongoDB, time series database CTSDB, and

Data transfer services, data backup services, intelligent DBAs, etc.

As the core product of the cloud, the database TencentDB ensures customer data security from below aspects:

- **Database Instance Isolation:** Through strict permission management measures, it ensures internally neither the operation and maintenance nor R&D personnel can log in to the database machine directly via other Tencent Cloud machines.
- **Database Authentication and Access Control:** Tencent cloud database instance access has strict identity authentication and access control measures.
- **Access Security and Data Encryption:** Cloud Database provides industry-leading secure access solutions and data encryption capabilities. The relevant solution keys are all securely stored in the KMS key.
- **Security Auditing Capability:** Provides a comprehensive security auditing and risk control mechanism that covers every operating system user and database user on the server; the audit records include the date, time, type, subject identification, object identification, and results of the event; The audit records are kept for more than 1 year and are stored in a higher security level to avoid unexpected deletion, modification or coverage.
- **High service availability and high data reliability:** Tencent Cloud guarantees high availability of database products through dual-IDC backup in the same city, automatic detection and automatic fault recovery, and second-level switching according to different database products. At the same time, we also provide automatic full-size backup and incremental backup, dual-living in the same city and other solutions to ensure that even if the hardware of the instance is faulty at the same time, the data can be recovered through the cold standby file.

6. Data Security

Is my production data safe on Tencent Cloud?

Is my personal data during registration and usage well protected?

In order to better secure my data, are there any recommendations for data management?

6.1 Secure Data in Cloud

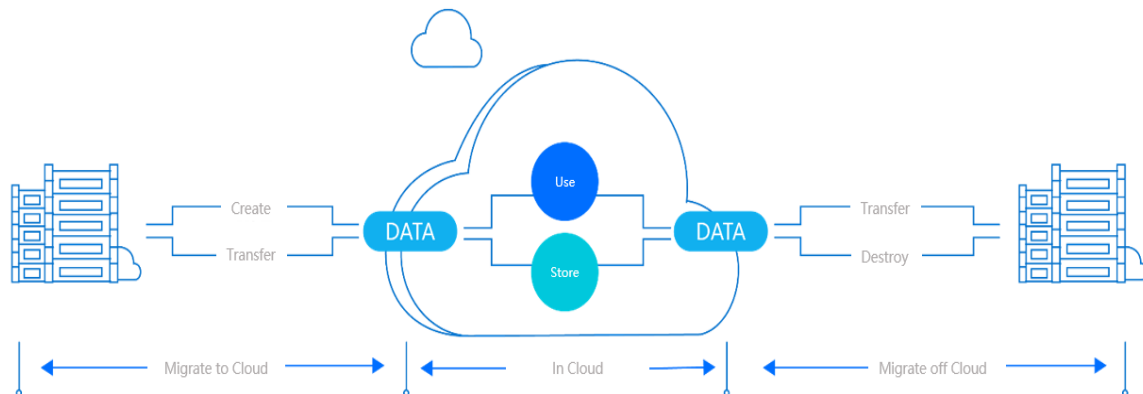


Figure 14 Simple Diagram of Cloud Data

When customers choose to use cloud products and services as the technical support for business operations, they will inevitably place relevant data in the cloud computing environment of public cloud service providers. In general, customer data goes through three main phases: Migrate to Cloud, in cloud and Migrate off cloud. The focus of customer data protection is different in each phase.

By developing leading security technologies and a comprehensive security management system, Tencent Cloud as a public cloud service provider ensures that your data can be free from issues that affect data confidentiality, availability and integrity due to the Tencent cloud platform. Additionally, Tencent Cloud recommends that all customers should ensure the security of data, applications, endpoints and accounts by deploying effective controls. Some of the best practices for data protection will be introduced in Section 6.2 of this chapter.

6.1.1 Data Protection in “Migrate to Cloud” Phase

The “Migrate to Cloud” Phase is the process of migrating the necessary business data/production systems to the cloud product after the customer purchases the cloud product and performs appropriate development, testing, and configuration. In this process, you can choose the appropriate data transmission method and transmission protocol (such as HTTPS, SSH, etc.) according to your security requirements and actual management and control capabilities. At the same time, you can choose the following network service products provided by Tencent Cloud to achieve higher security protection level:

Tencent Direct Connect is a dedicated network provided by Tencent Cloud and operator partners. Private line access ensures that data communication between your enterprise information center and the public cloud computing environment is always in an independent network link, realizing the isolation from other Internet traffic in the physical layer and effectively defending against network eavesdropping, network sniffing, network interception, network tampering and other attacks. Its high security and high stability can meet the regulatory and compliance requirements of financial industry, government and enterprises.

Tencent Cloud IPsec VPN can provide customers with a secure transmission network upon the Internet. The pre-shared key with IKE protocol is used for link encryption, which can meet the network security requirements in most cases. Additionally, Tencent Cloud IPsec VPN has a gateway layer dual-system hot backup configuration and allows multiple VPN gateways to be configured to achieve secure network access with higher bandwidth.

You can create new data directly in “Move to Cloud” phase. When you create it, you should refer to your company's established data classification and rating standards to assign new data the corresponding importance level to determine how the data is used, where it is stored, and whether encryption is needed when it is in storage.

6.1.2 Data Protection in “In Cloud” Phase

The “In Cloud” Phase is the process by which customers use their deployed cloud computing environment for business production activities. In this process, a large amount of sensitive data such as user information, business resources, and cache files are processed. Therefore, a complete security management mechanism is required to ensure the security of the data itself in the cloud environment.

Your business data is of the highest confidentiality level of in Tencent Cloud, and it is solely owned by yourself. Tencent Cloud has established a detailed data classification management standard and designed complete authentication and access control capabilities in the physical, network, system and application layer, together with the abnormal behavior monitoring mechanism based on big data to protect your business data against unauthorized access and destruction. At the same time, with the help of automated, instrumented operation and maintenance management tools, any Tencent Cloud internal staff will not be able to access your cloud business data without your authorization.

Every public cloud customer shares the underlying physical hardware provided by Tencent Cloud. Through strict development and design, Tencent Cloud ensures effective logical isolation of business data and production environments among different customers, including virtual machine image isolation, database instance isolation, private network access isolation, and object storage file isolation, etc. If your business requires a higher level of security, Tencent Cloud can also provide a cloud product¹ with exclusive host resources or you can purchase a cloud-based physical server directly².

Tencent Cloud utilizes a variety of security technologies and management tools to help protect your data. Using the anti-DDoS abilities provided by Tencent Cloud and with the help of multi-layer security mechanisms such as intrusion prevention, DNS hijacking detection, website security protection, virus/Trojan protection, your cloud data will be free from the malicious Internet attack. At the same time, according to the characteristics of each cloud product, Tencent Cloud adopts real-time hot standby, redundant storage and

¹ CDH (Cvm Dedicated Host): dedicated host allows you to purchase and create cloud hosts with exclusive host resources to meet your requirements on exclusivity, security and compliance; After purchasing a dedicated host, you can flexibly create and manage exclusive cloud hosts with customized specifications. For more information, please visit Tencent Cloud official website or consult sales staff.

² Blackstone Physical Server CPM (Cloud Physical Machine) is a physical server rental service that can be purchased on demand and paid for by volume. For more information, please visit Tencent Cloud official website or consult sales staff.

multi-site backup of master-slave data to ensure your business data is safe, reliable and continuously available.

6.1.3 Data Protection in “Migrate off Cloud” Phase

When you make business changes or needs to temporarily leave the public cloud computing platform due to a change of the IT plan, you can choose to perform backup migration of cloud data and production environment at any time. Tencent Cloud products allow you to back up and migrate your data in a common standard format, and you can use the same transmission method and transmission protocol as the “Migrate to Cloud” Phase, or use Tencent cloud leased line access, IPsec VPN and other network service products to ensure your data is safe and reliable in the next cloud phase.

When your public cloud service is terminated, Tencent Cloud will follow a strict data erase method to completely delete all your data before recycling your previously purchased computing and storage resources.

6.2 User Data Protection Practice

Helping customers to achieve better security compliance is one of the core values of Tencent Cloud. Tencent Cloud recommends all customers should design effective control measures to further improve data security in the cloud computing environment, according to their actual situation and security requirements.

Tencent Cloud will introduce ways to better protect your business data from the perspective of three key aspects: *authentication information, business data and log information*.

6.2.1 Authentication Information Protection

As the key to obtain data, authentication information could prevent customer data from being accessed and used without authorization. Therefore, authentication information protection should be one of the key security management measures of customers in business operations.

Tencent Cloud ensures that the authentication information you created/modified in the console is securely encrypted and stored in the cloud environment. However, you are strongly recommended to carefully distribute, use, and destroy business-related authentication information to prevent your data from being misused or stolen. Tencent Cloud recommends:

1. Avoid transmission of critical authentication information in clear text via channels such as email, websites, instant messaging, and paper.
2. Avoid using a shared account, at the same time reclaim account with the highest privilege, and create different account information according to the principle of minimum privilege and business needs.
3. When using password as the authentication information, the password should have a certain complexity and be replaced regularly.

4. Utilize multi-factor authentication method¹, such as using dynamic password or One-Time Password (OTP) to perform two-factor authentication.
5. Erase verified or invalid verification information in a timely manner.
6. Record complete authentication information usage records, periodically analyze abnormal usage records or set real-time warning thresholds.

The types of authentication information provided by Tencent Cloud for customers include:

- **Account Password:** Tencent Cloud provides multiple account management functions, and cooperates with strong password security policies to prevent attacks such as brute force attacks.
- **Two-Factor Authentication:** Tencent Cloud provides dynamic password verification capabilities to ensure account security when performing sensitive operations (such as deleting instances).
- **SSH key:** Tencent Cloud provides SSH secure login based on public and private keys, which is more secure than ordinary passwords.

6.2.2 Business Data Protection

Tencent Cloud will not touch or know the customer's content within the cloud environment. The customer content is defined as top secret by Tencent Cloud. No one has access to it without customer authorization, internal approval and corresponding technical support. For the management and protection of business data on the cloud, Tencent Cloud recommends that each customer define and enforce protection of business data on the cloud according to its own applicable security standards (such as ISO/IEC 27001: 2013, ISO/IEC 27017: 2015, level protection requirements, etc.) as well as the established security protection mechanisms, which include but not limited to:

1. Effectively identify business data on the cloud and classify data in a manner consistent with the security requirements of business operations.
2. Upon the completion of data classification, define and assign corresponding importance levels (or risk levels) to different categories of data.
3. Continuously update asset information, if necessary, establish a cloud data asset management system or connect with existing enterprise internal asset management systems.
4. Different data security rules are formulated for data information of various importance levels. Data information of higher importance levels should adopt stricter and more secure protection measures, such as data storage encryption, database table encryption, and transmission encryption. However, please note that both encryption and decryption require a certain amount of time and computing power, so data encryption may affect the efficiency of data usage. On the other hand, if the customer chooses to encrypt the business data, the key needs to be systematically and properly managed.

¹ Multi-factor authentication (MFA) is an access control method. Users could enter system or use resources only after successfully submitting two or more types of authentication information. The authentication information generally includes two or more of the following three types of information, namely, 1. Something they know, 2. Something they have, or 3. Something they are. For example, the password set by users is something they know, and the dynamic password token or the mobile phone dynamic password can be regarded as something they have, and the biometric authentication information, such as fingerprint or iris authentication, belongs to something they are. Some people also refer to the authentication method that only contains two types of authentication information as two-factor authentication, that is, 2FA (Two-factor authentication).

5. When accessing business data through the Internet, it is recommended to restrict access sources and targets by deploying firewalls, intrusion prevention systems, and anti-denial service systems. When customers expect to connect the purchased public cloud platform with the enterprise internal network, Tencent Cloud strongly recommends secure connection methods (such as VPN, leased line, encrypted link, etc.) to ensure that there is no Internet access gap in the internal network of the enterprise due to unsafe links;
6. Properly utilize Virtual Private Cloud products provided by Tencent Cloud to design and plan security zones inside the cloud computing platform. Private network functions can be used to implement security partitioning and access isolation in different logical areas such as core production, operation and maintenance management, development and testing, and external interaction.

6.2.3 Log Information Protection

Tencent Cloud is responsible for analyzing and processing non-user-level log information generated by the underlying public cloud products, which includes physical environment facilities, network equipment, server hardware, virtual control layer operating systems, and database management systems. As a user of Tencent Cloud Public Cloud products, you should pay attention to all log information (access records, operation logs, system status information, alarm information, error reminders, etc.) generated in the business operations activities for better safety control and risk disposal. We recommend:

1. Properly utilize the log recording function provided by Tencent Cloud to realize real-time monitoring of cloud product operation and access.
2. Set effective log management function for systems deployed on cloud products, such as operating systems, applications, database instances, etc.
3. Set up a centralized log collection and analysis system with security hardening and access control, and store separately or encrypt logs according to the sensitivity of the log information.
4. Strictly restrict access to log information. Secure connection (such as VPN, leased line, encrypted link, etc.) should be used for Internet transmission to ensure that the log information is not lost or tampered.
5. When conditions permit, you can deploy bastion hosts to obtain entire operational record, which could help your business achieve problem traceability and behavioral audits.

7. Operation Management Security

How do I monitor cloud product status?

I encountered a problem using cloud product, how can I get assistance? Is timely assistance available?

7.1 Tencent Cloud's Operational Management Capabilities

Your data will benefit from the underlying security capabilities offered by Tencent Cloud, as well as comprehensive business operation security. With many years of experience in security operation and a large service team, we can provide a wide range of operational support services including system process and change, account and access permission, monitoring and auditing.

7.1.1 Process Management

Behind every cloud product provided, Tencent Cloud is committed to incorporating ISO/IEC 20000 Information Technology Service Management standards and ISO/IEC 9001 Quality Management System standards into the entire product SDL security development process, focusing on requirements, design, development, testing, delivery, operation and maintenance, as well as other aspects. Information security and privacy issues are eliminated throughout the entire product development lifecycle to ensure that all cloud products have adequate security controls and assessments throughout their lifecycle:

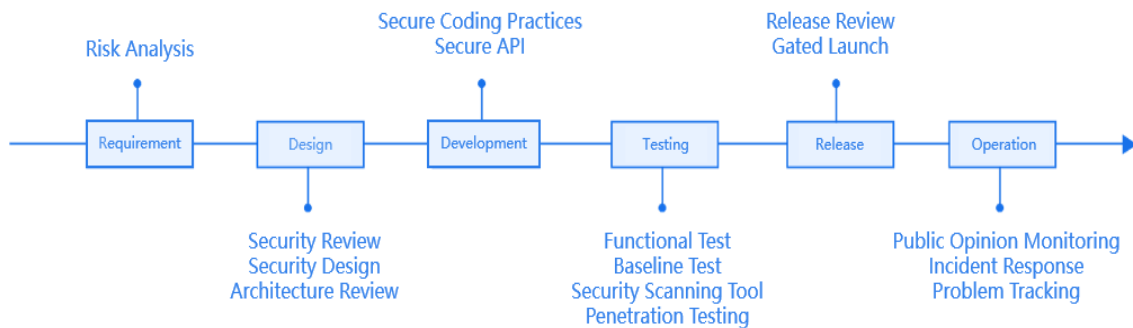


Figure 15 Diagram of Tencent Cloud Secure Development Process

To ensure the end user security, Tencent Cloud develops cloud platforms and cloud products in strict accordance with the security development life cycle approach, with the goal of incorporating information security into the software development lifecycle of the entire Tencent Cloud. Our software development lifecycle mainly includes:

- **Security Training:** To enhance the awareness of developer in security programming and strictly require relevant personnel to follow the security coding guideline.
- **Requirements Analysis:** Communicate on business content, business process, technical framework, and find the best way to embed security.
- **System Design:** Use threat modeling for system design and make security technology assessment of the adopted architecture.
- **Implementation:** In the development process, Tencent provides self-designed security development components for developers to use.
- **Verification:** Vulnerabilities are revealed through penetration test and code review.
- **Release:** The system can only be published to an online environment after the final review by the information Security Department to prevent the product from carrying security vulnerabilities when operating in the production environment.

Tencent Cloud Operations Service team is remodeling the operation process into management model, and has realized highly automated service delivery, control, release, solution and relation processes. In specific process management process, Tencent Cloud combines different standardized tools to enable automatic input/output, collaboration and integration for different operations processes. Automated process not only cuts down the overall operating costs, but also reduces security risks associated with manual errors and malicious operations. With automatic process alert control, error and failure will have quick alerts and reparation.

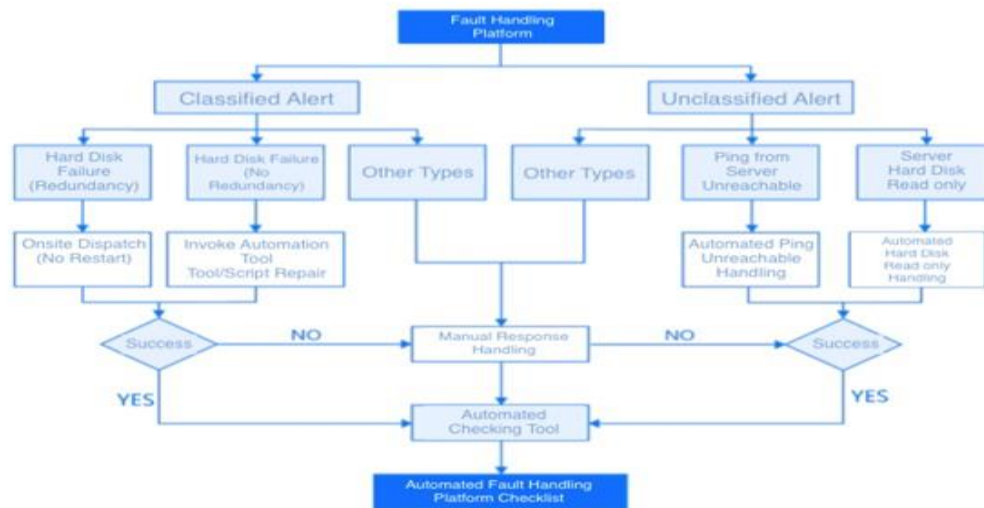


Figure 16 Diagram of Tencent Cloud Fault Automation Response and Processing

7.1.2 Operation and Maintenance Management

Tencent Cloud handles more than 12 million operation and maintenance requests on average per year, and strictly controls the change time window through the internal operation and maintenance management mechanism. All operation and maintenance requests can be completed within the specified time. With mature automated/tool-based operations management platform the massive operation maintenance operations are turned into a well-organized routine work, so that cloud products in functional iterations, patch upgrades, bug fixes and other key aspects can continue to provide risk-free, uninterrupted business operation and maintenance support.

Regardless of the cloud product types purchased, your business data is protected at the highest level within the Tencent Cloud. Tencent Cloud provides a complete operation and maintenance security mechanism to ensure that the Operations Service team cannot access your information assets directly without your consent and authorization. At the same time, Tencent Cloud has set up detailed operation and maintenance security responsibility boundary lines, and regularly perform internal operation and maintenance security review. An audit team of security experts issues and traces the risk alarms and suspicious operations in the operations process based on customized cloud security control activity items and practical experiences.

Additionally, the Tencent Cloud has an impact rating based on attributes such as the importance/urgency of the operations request and the extent of the change. In response

to the high impact operation and maintenance changes, the change notice will be timely published through the official website, forum and other channels. The likely affected customers will be notified about the change via SMS, mail or phone, so that you can better coordinate your business resources.

7.1.3 Permission Management

In the operation of cloud products, Tencent Cloud provides mandatory, fine grained rights management capabilities. In combination with the automated operation and maintenance management mechanism, Tencent Cloud has established a unified operational management portal, and all production environment operations are subject to strict permission control and monitoring.

Each member will receive a rigorous background check and competency assessment from Tencent Cloud before joining the operations management team, and only candidates who meet all the necessary requirements can officially become employees of the Tencent Cloud. Tencent Cloud will arrange suitable jobs and license according to the skill category and technical level of the employees, and provide comprehensive in-house training to help employees improve their working ability and professionalism. Tencent Cloud has designed a comprehensive information security training system to ensure that employees are constantly enhancing their security awareness and security technology upon onboarding.

The staff changes of Tencent Cloud operations management team are controlled by the unified Operation Management Portal to achieve automatic permission control: assigns basic default permissions automatically when onboarding, modifies permissions automatically when transferring, and disables all permissions automatically when leaving. Employees can request temporary or fixed permissions in the unified operations portal, and the system automatically assigns them new permissions after multiple levels of review and approval. Temporary permissions are automatically disabled after the end of the service period.

Tencent Cloud does not allow any potential conflicting permissions to be acquired at the same time with the help of the complex permission separation matrix mechanism in Tencent Cloud. Tencent Cloud regularly organizes internal permission audit to ensure that permissions are not abused or misused.

7.1.4 Monitoring and Auditing

Tencent Cloud enables comprehensive automated monitoring of all internal operations through big data processing and visualization analysis. The monitored objects include all backend system components such as network equipment, physical servers, databases and management systems, virtualization control layer, critical application services, etc., and the alarm threshold can be set based on different functions and usage of the system components. Once there is alarm triggered, the relevant personnel are notified for evaluation and handling.

Tencent Cloud production environment has fully deployed bastion hosts, and centralized control of the administrator account permissions of the Tencent Cloud backend system components through bastion hosts. Operations Management team members can only use the new account given by the bastion host and pass the second authentication (e.g.

dynamic authentication password) to login and get the appropriate system operation permissions automatically. All backend operation and maintenance records are encrypted and stored in the centralized log platform and are regularly audited by the internal audit team of Tencent Cloud.

7.1.5 Service Support

Tencent Cloud's comprehensive operational security capabilities can provide 24-hour technical support for cloud products.

Tencent Cloud has multi-regional customer service centers that can handle your advice and consultation 24/7. In addition to standard services, we ensure one-to-one expert service for large customers or special customers so that you can better utilize the cloud products provided by Tencent Cloud.

Tencent Cloud concerns about the customer experience. In order to have better understanding of your needs and meet your requirements, Tencent Cloud proactively obtains feedback from multiple channels:

- **From the regulatory body:** Through cooperation with local authorities, network supervision bureau, security notices related to Tencent Cloud itself or your business activities are obtained in a timely manner.
- **From internal feedback:** Tencent Cloud has established a public opinion monitoring system that can receive immediate security issue feedback from internal staff.
- **From the Internet:** Tencent Cloud Customer Service Center monitors Internet information channels such as V2EX and Weibo.

Tencent Cloud Customer Service Center provides you with industry-leading service response time and processing quality to ensure a successful resolution rate of 95% on the day you make a request or enquiry. Your satisfaction is the unrelenting pursuit of Tencent Cloud. The Operation Management Team works together with Customer Service center and can achieve up to 99% of customer satisfaction throughout the year.

7.2 Customer-facing Operational Management Products

Tencent Cloud assists you to manage your business activities in real time. All purchased cloud products can be monitored and managed through the Tencent Cloud Web Console. The web console provides you with cloud platform operation and maintenance functions such as cloud account management, access rights settings, product function configuration, network configuration, health status and security status monitoring, alarm settings and log management.

7.2.1 Cloud Monitoring

Cloud monitoring services can be configured in your cloud computing console. The basic monitoring function with minimal manual intervention through intelligent data analysis, real-time fault alarm and personalized data report configuration can well cover all cloud product health indicators (such as cloud server CPU utilization, memory utilization, disk utilization and cloud database, Memcache high-speed storage and other cloud service

loads) and performance indicators, providing you with high-transparency of data monitoring for cloud products. The basic monitoring functions can support abnormal alarm settings of multiple products, multiple strategy and multiple notification channels. It not only allows you to know your business status in the first time, but also triggers resiliency capability through monitoring to ensure that automatic performance expansion can be implemented when the risk indicator reaches the pre-configured alarm triggering condition, in order to meet requirements of business operation availability.

- **Daily Inspection:** Provide visual chart analysis for daily inspections, which is convenient for monitoring, comparing and detecting abnormalities.
- **Anomaly Locating:** Quickly define the range of anomalies and find out the cause of the anomaly. You can compare data of any two periods of time to help troubleshoot the fault.
- **Alarm Notification:** Provide alarm notification to inform the recipient immediately.

Additionally, custom monitoring function will further help you to define the metrics of the cloud products what you have purchased. Tencent Cloud provides you with a simplified operation management mode. You can customize the relevant indicators and report them to the console according to different business needs without complicated coding and additional capital investment. You can know the quality of the service in real time and discover important system abnormalities in advance to achieve business operation refinement.

7.2.2 Cloud Automated Testing

In order to help customers to better monitor the availability and stability of their global business, cloud automated testing, as Tencent Cloud's proprietary inspection network for service quality, can be used for every minute periodic monitoring of your website, domain name, backend interface, etc. in various business scenarios, assisting you to respond to abnormal status in a quickly manner.

- **Site Automated Testing:** Provides a comprehensive view of website access availability and latency based on monitoring sites of more than 20 major national provinces and mainstream operators. The alarm threshold can be set and there will be real-time alarm notification once triggered.
- **Service Port Automated Testing:** Supports periodic continuous access to any TCP port, monitors the status of the port and can configure automated testing for multiple protocols such as HTTP/HTTPS, TCP, and PING.
- **Domain Name and IP Connectivity Automated Testing:** The domain name is periodically detected through PING and the automatic detection cannot be lower than the connectivity with the operator.

7.2.3 Cloud API

As the cornerstone of Tencent Cloud's open environment, the Cloud API can cover all cloud products that can provide services to external in this way and it is continuously iterated, so API interface security becomes extremely important.

A typical API interface request is as follows:


```
https://cvm.tencentcloudapi.com/?Action=DescribeInstances
&Filters.0.Name=zone
&Filters.0.Values.0=ap-guangzhou-1
&Filters.0.Values.1=ap-guangzhou-2
&Offset=0
&Limit=1
& <Common request parameter>
```

Figure 17 Diagram of Tencent Cloud API Interface

Remark: Action=DescribeInstance means to query details of cloud server instance

For more details, please refer to <https://cloud.tencent.com/document/api/213/15728>

Tencent Cloud provides you with Cloud API that supports HTTPS transmission encryption, realizes interface authentication through various SDK signature mechanisms (such as PHP, Python, Java, .Net, Node.js, etc.) and uses Timestamp to limit the validity of request signatures to prevent replay attacks. In the meantime, the signature encryption not only supports HmacSHA1, but also supports more secure HmacSHA256 to ensure the security and legality of API requests.

While providing cloud API security capabilities, Tencent Cloud integrates cloud API monitoring and management functions. You can set the API interface status monitoring through the console based on your business requirement. At the same time, Tencent Cloud provides you with API interface protection capability, which can effectively eliminate the risk of cloud API failure or abuse.

7.2.4 Access Management

Cloud Access Management (CAM) is a set of permission management tool provided by Tencent Cloud to help customers securely manage access, resources and use of Tencent Cloud accounts. With CAM, you can create, manage, and destroy users (groups) and control who can use Tencent cloud resources by identity management and policy management.

- **Administrative Access Right:** You can authorize other people to access the resources of the primary account without sharing the identity credentials associated with the primary account.
- **Grant Fine Permissions:** You can grant different permissions to different people for different resources. For example, some subaccounts can be allowed to have read permission of a COS storage bucket, while other subaccounts or root accounts can have write permission of a COS storage object, etc.
- **Two-factor Authentication:** You can use secondary identity verification for the primary account and the subordinate sub-account to improve account security.
- **Federated Identity:** Users who have obtained passwords in a third-party authentication system (for example, in your enterprise network or through an Internet identity provider) can be allowed to have temporary access to your account in the cloud.

- **PCI DSS Compliance:** CAM supports the processing, storage and transmission of credit card data by merchants or service providers, and has been verified that it is compliant to the Payment Card Industry (PCI) Data Security Standard (DSS).
- **Most Tencent Cloud products are supported:** For a list of Tencent Cloud products that support CAM, please refer to products that support CAM.
- **Final Consistency:** CAM currently supports multiple regions of Tencent Cloud. Cross-region data synchronization is realized by replication policy. Although CAM will submit changes to the policy in time, the time when the policy take effect will be delayed due to cross-region policy synchronization. At the same time, CAM uses cache to improve performance, which may increase time consumption in some cases. Policy changes may not take effect until previously cached data expires.

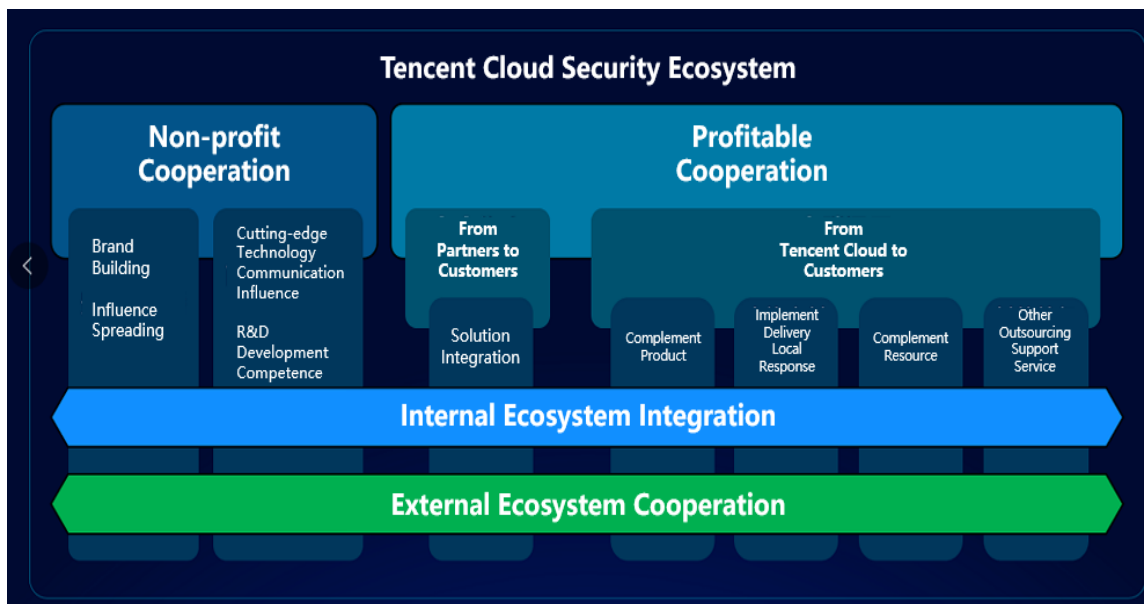
7.2.5 Cloud Audit

Cloud Audit is a service that supports regulatory and compliance checks, operation and risk audit of your Tencent Cloud account. You can log, continuously monitor and keep records of account activities generated from your account and corresponding sub-accounts. The event history of cloud audit records simplifies security analysis, resource change tracking, and troubleshooting work.

- **Simplify Compliance:** With cloud audit, you can easily record and store event logs for accounts and sub-accounts that have been executed on the Tencent Cloud API or Tencent Cloud Console in the last 7 days, simplifying compliance check.
- **Tracking Set:** A tracking set is an enhancement to an operation record. Through the tracking set, you can trace historical events, including operation log type information, operation log storage path, and so on.
- **User and Resource Activity Visualization:** Cloud audit visualization records Tencent Cloud Console operations and API calls to improve user and resource activity.
- **Security Analysis and Troubleshooting:** With cloud auditing, you can discover and resolve security and operational issues by querying the overall history of changes to accounts and sub-accounts during a specific period.

8. Tencent Cloud Security Environment

Information security in a cloud computing environment can no longer be achieved solely by relying on a certain type of technology or some talents. Like the “open” feature of cloud computing itself, cloud computing service providers must effectively integrate internal and external resources to achieve a win-win development goal in order to build a complete and robust cloud security environment for Tencent Cloud’s customers.



8.1 Internal Environment - Resource Integration, and “Cloud, Channel, Client” Security System Building

As one of the world's largest Internet companies, Tencent understands the security issues that companies concern the most. Relying on the overall deployment of Tencent's “Cloud, channel, client”, the seven types of cutting-edge technology of laboratories, the 20 years of security capabilities and the strong support of massive data, Tencent Cloud is committed to providing global security solutions for the entire security environment.



Figure 24 Advantage of Tencent Cloud Security

Three Aspects of Management – “Cloud, Channel, Client” Comprehensive Protection

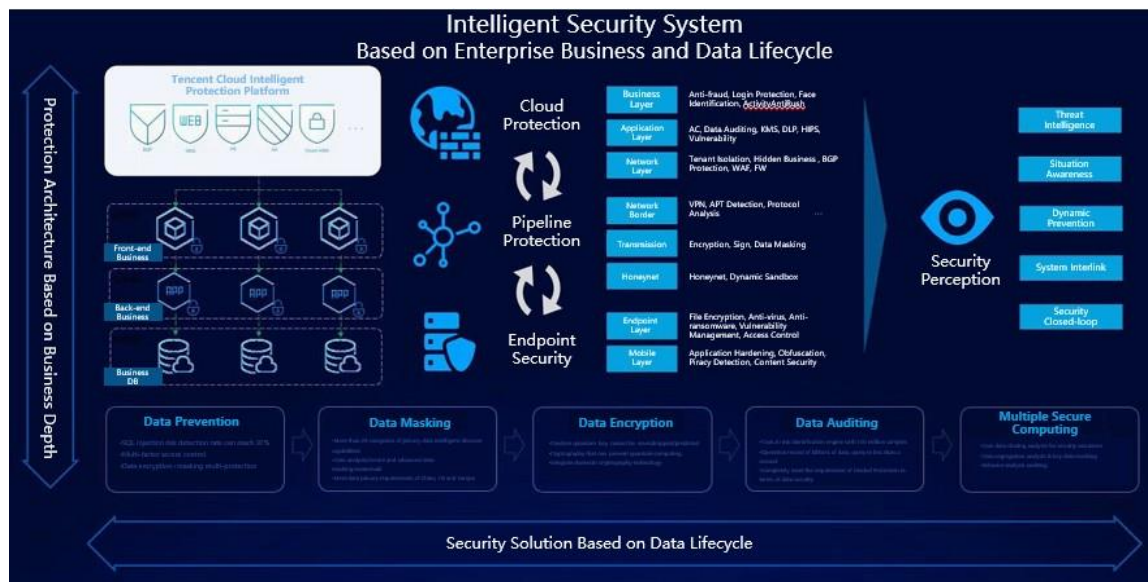
With the maturity of cloud computing technology, Tencent has been committed to building a “Cloud, Channel, Client” Internet industry environment platform.

Tencent Cloud leverages Tencent's rich resources and powerful computing capabilities to perform the fastest threat detection and provenance analysis to help the entire security environment. Additionally, with the increasing use of cloud computing in various industries, Tencent Cloud also protects enterprise cloud deployments, providing comprehensive security protection from network, host to data and business security.

boundary is an important channel between company's internal and external networks, and its security is essential. Based on the core technology of HOB0 analysis system¹, combined with big data and deep learning, Tencent Cloud can effectively detect unknown threats. It can also analyze the network traffic at the boundary of the internal and external networks of the enterprise to discover vulnerability exploits and attacks and accurately detect advanced threats.

In terms of the endpoint, Tencent applies the tens of billions of cloud anti-virus database, engine library and Tencent TAV anti-virus engine, and system rectification engine to the enterprise, which can effectively defend against Trojan on intranet endpoints. Tencent's endpoint security management system integrates security management functions such as unified endpoint anti-virus management and control, unified vulnerability rectification management and control, and policy management and control. Relying on Tencent's terminal protection capabilities, Tencent Cloud can help enterprise managers fully understand and protect enterprise endpoint security.

Under the comprehensive deployment of "Cloud, Channel, Client", Tencent Cloud fully integrated internal resources into the development of enterprise security environment.



¹ HOB0 Analysis System is a self-developed security assistant platform of Tencent Anti-Virus Lab, which has accurate identification, rapid response and network-wide monitoring capabilities. Relying on massive analysis clusters, intelligent detection technology that is based on big data processing and the industry's top anti-virus analysis team's three "magic weapons" to protect users cybersecurity.

Seven Major Labs – Top International Research Team

Tencent Security United Laboratory covers seven major laboratories: Anti-Virus Lab, Anti-Fraud Lab, Mobile Security Lab, Keen Security Lab, Xuanwu Lab, Zhanlu Lab, and Yunding Lab, focusing on building security attack and defense system. The security protection and assurance scope covers six key areas of the Internet: connection, system, application, information, device and cloud. With an open mind, Tencent Security United Laboratory brings together many of the world's top white hat hackers and continues to provide technical output for the Internet security industry. The united laboratory is one of Tencent's core competitiveness.

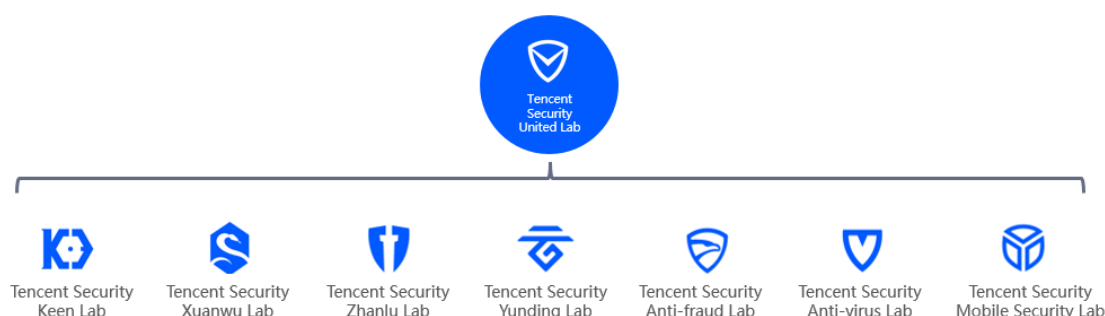


Figure 25 Tencent Security Laboratory Diagram

20 Years of Experience – Accumulated Security Capabilities

Tencent has 20 years of experience in the security field, constantly absorbing cutting-edge technology and developing comprehensive security capabilities.

In order to help customers to deploy cloud services more securely, Tencent Cloud has accumulated comprehensive security capabilities such as host security, DDoS prevention, and web application firewall. Additionally, facing new challenges to enterprise data security brought by rapid development of cloud computing IoT and AI technology enterprise data security, Tencent Cloud with its years of experience in data protection, has created a data-centered full-process protection solution - Data Shield. It builds a one-stop full-process protection system through data auditing, privacy protection, threat defense, quantum encryption and other products. Additionally, Tencent has strong data cleaning capabilities to ensure the integrity and accuracy of enterprise data. With the increasingly close relationship between enterprise security and business, Tencent Cloud relies on Tencent's extensive business data and collected cyber black-market intelligence to accurately identify potential business security risks and protect enterprises from financial loss.

In terms of the network border, Tencent Cloud can adopt virtual execution technology based on Tencent's HABO sandbox analysis to perform asynchronous concurrent analysis and processing on the files extracted from boundary traffic analysis. A real physical server can simulate dozens of virtual machines and support flexible horizontal

expansion to cope with high concurrent business needs. It can achieve real-time alarm, anomaly recovery and stable operation in unsupervised mode. Additionally, it also has the capability of network traffic detection, mail gateway detection, GAP and APT protection.

With the increasing popularity of mobile endpoint devices, Tencent Cloud also has comprehensive mobile security protection capabilities, covering application hardening, vulnerability scanning, piracy monitoring, real machine testing, quality tracking, secure payment and other scenarios.

8.2 External Environment - Cooperation with Multiple Parties to Establish an Open, Coordinated and Win-Win Security Environment

We stick to the “Sharing, Jointly Building, and Win-win” principle, continue to build a new harmonious and robust enterprise security environment, and work together with partners to promote mature and lively security development. We try to build a secure and valuable Internet environment in terms of industry development, technical capability, market operation, etc.

- **Shared market opportunities:** Tencent Cloud provides a number of market opportunities for security environment partners. First, the security environment partners can use Tencent Cloud Market to display their products, solutions and services, and share the potential customers and sales opportunities of Tencent Cloud, improving the efficiency of product sales operations and reducing costs. Second, Tencent's cloud service resources are spread all over China and around the world. Security environment partners can use the Tencent resource network to rapidly deploy their business globally. Third, Tencent Cloud has established extensive cooperative relationships with the government, education, medical, manufacturing, energy, transportation and major enterprises. Partners have the opportunity to share relevant market resources. Tencent is always willing to promote the win-win of customers, partners and Tencent.
- **Provide technical support:** Tencent Cloud opens the cloud technology service interface to the security environment partners, and empowers its partners to help partners achieve business success. At the same time, Tencent Cloud will share security technology capabilities and security engineering capabilities with security environment partners, to generate security experience and share security resources. Tencent will empower partners to help them improve their security capabilities in various ways, including training, certification, interface development, technical documentation, security standards, process specifications, security testing, etc.
- **Security consulting services:** Tencent Cloud has established in-depth cooperation with internationally renowned consulting organizations to help users design industry security solutions and business models to accelerate the digital transformation of the industry. At the same time, Tencent seeks to develop in-depth cooperation with outstanding manufacturers to develop security solutions for various industries, such as education, medical, manufacturing, energy, transportation, to achieve common good.

- **Open Resources in Cloud Environment:** In addition to security technology and cooperation with consulting services, Tencent Cloud proactively participates in and actively contributes to development cloud security standards and open source communities, contributing to the healthy development of the cloud computing industry. Tencent Cloud also provides a variety of basic capabilities and security services to provide security services for software and application developers.

Appendix

Appendix I: Tencent Cloud Privacy Statement (2018)

If you decide to use or continue to use our services, it is regarded that you give consent to the collection, use, storage and sharing of your information in accordance with *Tencent's Tencent Cloud Privacy Statement*.

View Privacy Statement: <https://intl.cloud.tencent.com/document/product/301/17345>

If you have any questions about the privacy statement or other related issues, please contact us at <https://console.cloud.tencent.com/workorder> .

Tencent Cloud



腾讯云