JuFeng BCloud365 Platform

Security White Paper

Version 1.0.202105

Contents

1. Bcloud platform intruduction

1.1 Jufeng intruduction

Founded in 2008, Hangzhou Jufeng Technology Co., Ltd. is a high-tech enterprise integrating production, sales and service with "R&D" as it's core. It is committed to provide high-quality, cost-effective security products and industry solutions. The company is headquartered in Building D6, iValley, No. 1 Jiulong Avenue, Yinhu Street, Fuyang, Hangzhou. After years of development, Jufeng has become a video surveillance product and solution provider with excellent reputation in China. For now, it has established branches in major cities in China, radiating across the country, and serving all customers .

Since its establishment, Jufeng Technology has been focusing on the field of video security and has core technologies and solutions with independent intellectual property rights. At the same time it persists in challenging new technologies and new methods. The company mainly provides network cameras, HDD video recorders, network video servers, video codecs, smart home application products, splicing screens, cloud monitoring platforms and other video surveillance equipment and overall industry solutions, covering road monitoring, smart transportation, urban security, vehicle monitoring, community monitoring, IOT and other fields. The products sell well in domestic and overseas markets and are exported to many countries, so that customers all over the world can experience the convenience brought by Jufeng.

With it's forward-looking innovative technology, Jufeng Technology has become a high-tech enterprise with extraordinary development potential in the industry. It has a number of independent intellectual property rights and related qualification certificates such as patents, software, trademarks, etc., and has been identified as Hangzhou Enterprise Technology Center and Hangzhou High-tech Enterprise R&D Center and won the title of China's Top 100 Security Network Enterprises. It is one of the recommended brands of China Safe City Construction and one of the members of China Security Products Industry Association, and listed as a national high-tech enterprise. The products have been awarded the title of Hangzhou Major Scientific and Technological Innovation Project and Zhejiang Province Industrial New Product. It also obtaines the Zhejiang Provincial Security Technology Protection Industry Credit

Rating Certificate.

1.2 Jufeng cloud platform (Bcloud)introduction

Jufeng Cloud Platform (BCloud) is developed based on the company's security monitoring products, providing safe, stable and fast video cloud services for Jufeng and its customers. Jufeng Cloud Platform deploys cloud services globally, with tens of millions of users and hundreds of millions of concurrent processing capabilities. At the same time, Jufeng Cloud Platform provides customers and manufacturers SDK for self-service software development and an open and complete cloud platform API. Accordingly, a debugging Demo is provided, which can minimize the manufacturer's development threshold, save development costs, and increase the manufacturer's product development speed. It can also help manufacturers upgrade their software and hardware, and continue to provide high-quality services to users.

Jufeng Cloud Platform (Bcloud Platform) is an unified platform for both customers (toC) and business(toB). Based on the years of experience accumulation and summary from Jufeng and its partners, it is continuously optimized and unified for different customer groups. The basic cloud platform service greatly facilitates the sustainability and compatibility of manufacturers' business expansion.

1.3 Information security commission

Jufeng is committed to providing customers with consistent, safe, reliable and legally required video and IoT access services, and effectively guarantees the availability, confidentiality and integrity of the data of customers and their users. Jufeng Cloud promises: Jufeng Cloud Platform (BCloud) takes data protection as the mission core, cloud security capabilities as the cornerstone,relies on Jufeng’s unique IoT solutions to gain industry-leading competitiveness,builds a complete cloud platform security system, and consistently regards information security as one of Jufeng Cloud’s important development strategies.

In order to achieve these goals, we have started security protection in various levels, including security inspections, security defenses, and security monitoring and auditing of all external services, forming a full-process protection before, during and after the event.

This white paper discuss different security protection solutions from below points:

1. Security responsibility
2. Compliance
3. Data security
4. Bcloud platform basic structure
5. Security organization and personel
6. Bcloud platform security guarantee
7. Security development stage management
8. Security operation and maintenance
9. Business security and risk control
10. Terminal security
11. Business sustainability

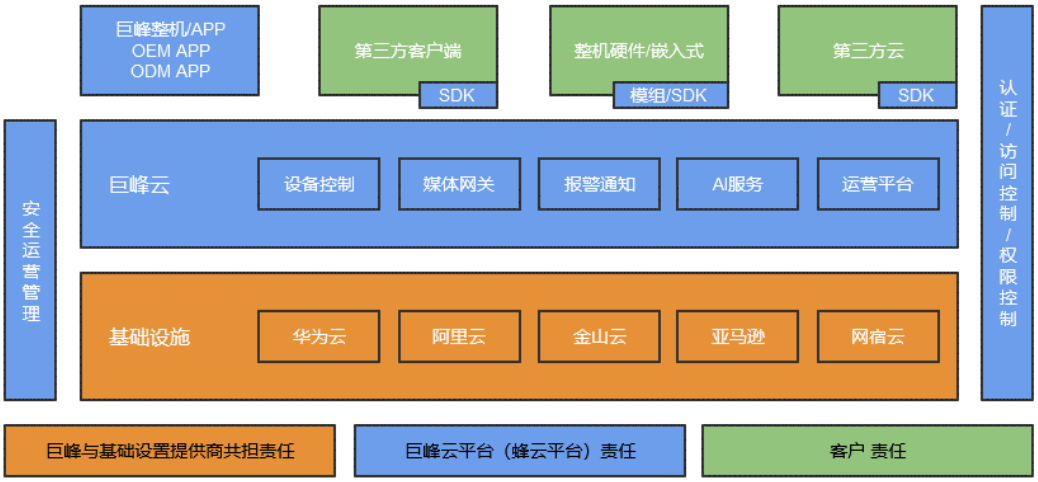
This white paper is dedicated to allow customers to have a more comprehensive and systematic understanding of Jufeng Cloud platform (BCloud), and to have deeper security insights into Jufeng Cloud Platform.

"Jufeng Cloud Platform (BCloud)" is hereinafter referred to as "BCloud Platform".

2. Security responsibility

Jufeng is responsible for the security management and operation of services and data interaction on the Bcloud platform, and is responsible for the security of the cloud service platform and basic structure provided. Customers who make self-develop apps or connect hardware embedded software to the Bcloud platform need to ensure that their application and data, including hardware and apps, are in compliance.

The picture below shows the shared responsibility model of information security of basic cloud service providers, Jufeng and customers.



2.1 Bcloud platform security responsibility

Bcloud platform selects the world-famous cloud hosting service providers Amazon, Huawei Cloud, Alibaba Cloud and other world-class cloud platforms to ensure the infrastructure and basic network security for security management and operation.

Bcloud platform security covers data security and cloud service security. Jufeng promises to use the professional anti-attack protection technology from its security team and well-known security service manufacturer around the world to provide secure operation and maintenance services of the cloud platform, which will effectively protect the security operation of Jufeng Cloud, and protect the privacy and data safety of customers and users. Mainly covering:

- Data security: which means the security management of the customer's business data in the cloud computing environment, including collection and identification, classification and grading, authority and encryption, and privacy compliance;
- Access control management: access authority management to resources and data, including user management, authority management, identity verification, etc.;
- Cloud service security: which means the security management of business-related application systems in the cloud computing environment, including the design, development, release, configuration, and application.

2.2 Customer security responsibility

When customers use the solutions of theBcloud platform, they need to strictly follow the security configuration and access requirements of Jufeng. At the same time, customers need to ensure the security of their own cloud, client or hardware products themselves. For APPs which developed based on Jufeng SDK, Jufeng only provides technical support and cannot provide any security guarantee. For data security compliance, privacy policy and other related information based on Jufeng OEM (public version) APP (without any customized scenarios), Jufeng will provide templates for customers'reference. The specific online privacy policy statement and legal compliance are made by customers. If necessary, Jufeng security team is willing to provide assistance and consulting services for security solutions.

3. Compliance

Jufeng complies with international authoritative safety standards and industry requirements, integrates them into the internal control framework, and strictly implements them in the process of realizing the requirements of cloud platform, app, hardware products, etc. Jufeng cooperated with independent third-party security services, consulting and audit institutions to verify and ensure the compliance and security of Bcloud365 platform.At present, Jufeng has passed the certification of information security and privacy compliance by multiple consulting and audit institutions around the world. It is an IOT solution provider with multiple certifications. Jufeng promises to continuously carry out multiple certification and compliance certificates related to information security and privacy security to escort customers' data and privacy security.

At present, our certification and compliance certificates are as follows:

3.1 ISO 9001

Jufeng cloud (Bcloud365 platform) has obtained ISO 9001 certification.

ISO 9001 is transformed from the world's first quality management system standard BS 5750 (written by BSI). ISO 9001 is a relatively mature quality framework in the world so far. It is a systematic guiding program and normative framework to ensure the product quality and operation of the company, focusing on the products or services provided by the enterprise. Plan, implement and improve the whole process of product or service realization to ensure that the requirements of customers and relevant laws and regulations are met. The application of quality management system can effectively and efficiently achieve the expected quality objectives. Take corrective and preventive measures through the audit and management review of the quality management system. Continuously improving the effectiveness of the quality management system is the foundation of enterprise development and growth.

3.2 ISO 27001

Jufeng cloud (Bcloud365 platform) has obtained ISO 27001 certification.

ISO 27001 is an international standard for information security management system (ISMS), which provides best practice guidance for various organizations to establish and operate information security management system. According to standard requirements:

- Establish, implement, operate, monitor, review, maintain and improve information security based on business risk approach;
- In order to ensure the confidentiality, integrity and availability of information, the corresponding organizational structure has been

established, a systematic security management system has been established, and resource guarantee has been provided;

- Follow PDCA method and continuously improve information security management.

4. Data Security

4.1 Data security system

From the perspective of data security life cycle, Jufeng cloud data security system adopts management and technology to carry out comprehensive and systematic construction. Through the data security management and control of all links in the data life cycle (data collection, storage, processing, transmission, sharing and deletion), the data security goal is realized.

At each stage of the data security life cycle, there is a corresponding security management system and security technology guarantee.

4.2 Data Ownership

In the services customized by Jufeng for customers, the customer is the data controller, and the customer needs to ensure the compliance of data use. Jufeng is the data processor. Jufeng will process the customer's personal data in accordance with the customer's written instructions and contract agreements on the basis of compliance with laws and regulations, and all data processing behaviors are transparent to the customer. Therefore, on the basis of complying with laws and regulations and privacy policy, Jufeng can help customers and users ensure the confidentiality, integrity and security of data.

4.3 Multi Replica Redundant Storage

The distributed architecture is adopted, and all business servers are deployed in three machine rooms in different areas of the same city at the same time. The data storage services such as database adopt the multi copy mode (at least two real-time copies are guaranteed), and data backup is carried out in real time. It ensures the high reliability and availability of data and services from the physical level.

4.4 User Device Data Security

The user device serial number is uniformly saved with the user system and can be obtained only when the user password is verified correctly. The device password of the mobile client will only be saved locally in the current client after the user enters it, and will not be synchronized or uploaded to the cloud. There is no possibility that the device password will be leaked in the cloud.

For ease of use, the cloud website will have the function of "remember password". Users can edit and save it voluntarily. After saving, users can clear and modify it at any time.

The signaling data interaction between the device and the client is not analyzed or saved in the cloud.

The video interaction data between the device and the client will be saved briefly in the ECS memory and will be released automatically after a few seconds.

4.5 Residual Data Removal

Once the host machine used by the Bcloud365 platform is released and recycled, all its information will be automatically overwritten with zero value. Meanwhile, any replaced and obsolete storage devices will be demagnetized and physically destroyed by the ECS infrastructure provider before they can be transported out of the data center.

4.6 Privacy Protection

Bloud365 platform practices the business philosophy of "everything depends on user value", and pays special attention to establishing a long-term and sustainable trust relationship with customers. Jufeng ensures the comprehensive protection of user and customer data with a solid technical foundation and complete operation management mechanism. Jufeng cloud will strictly implement the privacy policy published by Jufeng to effectively protect users' privacy.

- The main protection methods of cloud platform for private data are as follows:
- Privacy data production and classification
  - Basic principle:
    - Legal requirements for all acts of the information collection subject, including the authorization of the data subject and the clarification of legal responsibilities.
    - The principle of minimizing collected data does not collect data irrelevant to the services provided.

- Full users' right to know
  - Privacy policy of app and website
    - The privacy terms must specify the types of user data collected by the application and the corresponding services.
    - Privacy terms must be informed to users by email, APP pop-up window and other means at important times involving registration and update.
    - Privacy terms must include data collection, deletion, migration, saving, user options, etc.
    - Users are required to give feedback on the privacy policy.
  - Website cookie statement
    - The role of cookies and user choice.
- User rights:
  - Access rights
    - Jufeng users can access the personal data collected by Jufeng through the app without additional technical support.
    - Jufeng users can request Jufeng to inform them of the processing and use of their data
  - Forgotten right (data deletion right)
    - Account cancellation authority and data deletion
  - Right of correction
    - If you know that the personal information provided by the user is inaccurate or needs to be updated in time, you can modify it manually on the app.
  - Portable right
    - Users can send personal data supplied to Kyoho to another data controller through giant peak APP feedback or customer mailbox feedback.
- Data classification: distinguish between personal data and platform information data. For personal data, sensitivity classification is required

4.7 Data Storage Area

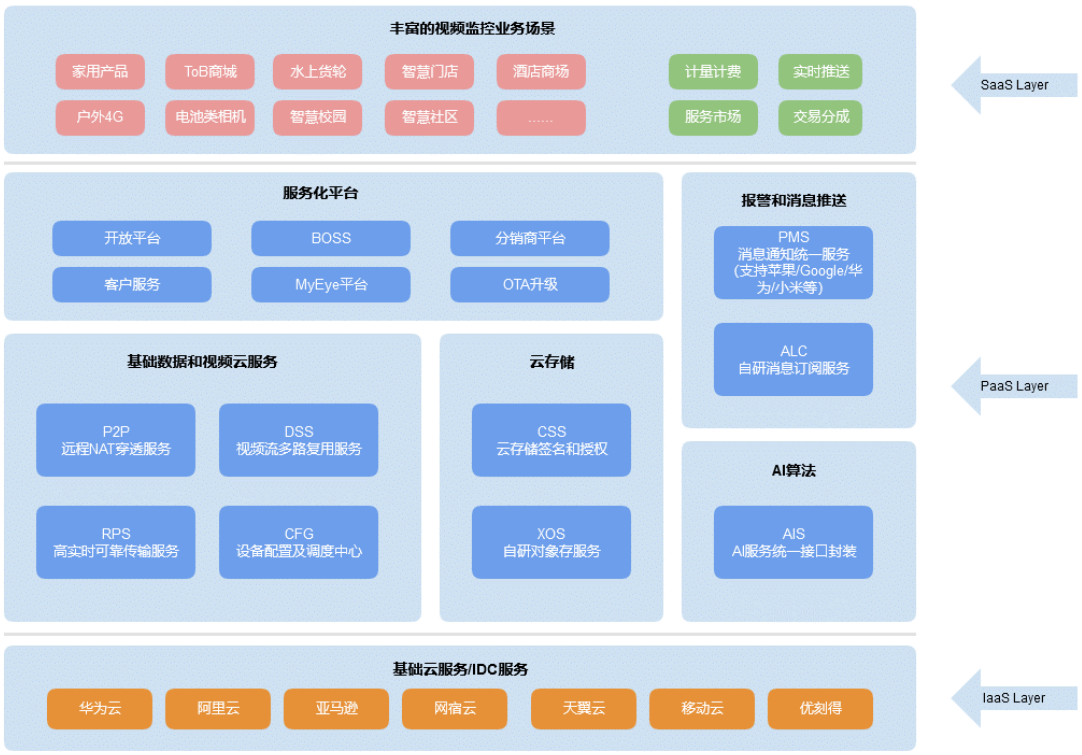
Four global clusters: China, North and South America and the Caribbean, Europe and Africa, and Asia Pacific region (including China Hongkong / China Macao / China Taiwan).Provide corresponding data services according to the user's local area.

- Mainland China: The data is stored in Huawei cloud - Guangzhou / Huawei cloud - Beijing 4 / Huawei cloud - Shanghai 2 computer room, and Huawei cloud provides basic cloud computing services; Alibaba cloud provides cloud computing services for Hangzhou computer room; Yangzhou computer room is provided with cloud computing services by nethost cloud;

- North and South America and the Caribbean: western United States - Oregon computer room / California computer room and eastern United States - Northern Virginia computer room, supported by cloud computing provided by Amazon (United States); South America - Sao Paulo, Brazil. Amazon and Huawei cloud jointly provide basic cloud computing services;
- Europe and Africa
  - EU countries: Computer room in Frankfurt, Germany, with computing services provided by Amazon;
  - Russia: Huawei cloud and Russian operator sbercloud jointly provide basic cloud computing services;
  - South Africa: Johannesburg computer room, with Huawei cloud providing basic cloud computing services;
- Asia Pacific: Computer rooms in Singapore / Hong Kong / India / Thailand / Vietnam / Philippines, etc. are jointly provided with basic cloud computing services by Amazon / Huawei cloud / nethost cloud / youkede, etc;

5. Cloud platform infrastructure

5.1 Cloud platform infrastructure diagram



The infrastructure of Bcloud platform is provided by Huawei cloud and Amazon, integrating global service nodes.At the service level, it provides customers and manufacturers with self-service software development SDK and open and perfect cloud platform API.

See open platform for details: https://open.bcloud365.net

5.2 Bcloud server supplier request

JFTECH requirements for cloud server providers.

1.Globally renowned cloud service provider brand with global leading technology level.

2.Cloud computing products are secure and stable.

3.Have and meet the most complete information security compliance, legal and qualification certificates worldwide.

Cloud server providers currently chosen by us, including HuaweiCloud, Amazon, AlibabaCloud, etc.

6. Security organization and personnel

6.1 Security and privacy teams and personnel

Internally, a Security Committee has been established with key founders leading the committee with key personnel from various departments such as Marketing/HR/R&D to provide risk and compliance support to JFTECH (including operational and business stakeholders) with a baseline of compliance with regulatory and compliance requirements.

The Security Committee has two departments under it, the Network Security Technology Center and the Security Emergency Response Center.

6.2 Human Resource Management

JFTECH's HR management framework is consistent with our company's overall HR management framework, which is based on the law. The main requirement for HR security is to ensure that our employees' backgrounds and qualifications are suitable for the needs of JFTECH's business. Employees behave in accordance with all laws, policies, procedures and the requirements of JFTECH Code of Business Conduct. Employees have the knowledge, skills and experience necessary to perform their duties.

When employees leave our company, there is a strict internal Task system process, and there are responsible persons in each link for the recovery or destruction of their electronic equipment, servers, various accounts and other resources, otherwise the separation procedures cannot be completed.

6.3 Safety awareness education

In order to enhance the network security awareness of all employees, avoid the risk of network security violations, and ensure the normal operation of business, JFTECH has issued the "Network Security Technology Center System" and "Network Security Technology Center Operating Procedures" internally, and the company has also promulgated the "Confidentiality System", and regularly conducts network security awareness education and learning based on this, requiring employees to

continuously learn about network security and understand the manual The policies and systems above. Know which behaviors are acceptable and which are not, realize that even if there is no subjective malice, they are responsible for their own actions and commit to perform as required.

6.4 Safety management system related training

In order to enable all members of our company to accurately understand the company's information security management policy, and to effectively promote and implement security policies, each year the company's security team and legal team conducts training on the company's information security such as "Confidentiality System".

6.5 Improvement of Information security protection ability

JFTech company inside regularly hold security development training and information security exchange to improve employees' security skills, ensure that employees can deliver safe and compliant products, solutions and services

7. Bcloud platform security guarantee

7.1 Physical security

7.1.1 Highly reliable basic structure

BCloud integrates the world's most well-known cloud hosting providers, including Amazon, Alibaba Cloud and Huawei Cloud, to build global service network. We provide customers with secure, stable, continuous and reliable physical facility base.

BCloud based on domestic and foreign sales areas, submarine optical cable distribution, and actual test results in various cities around the world. Deployed to cover available areas in China Mainland, Europe, Africa, Americas and Asia-Pacific region

- China Mainland:
  - Huawei Cloud(including but not limited):

        - Beijing Server Room 1
        - Beijing Server Room 4
        - Shanghai Server Room 1
        - Shanghai Server Room 2
        - Guangzhou Server Room
        - Guiyang Server Room
    - Kingsoft Cloud(including but not limited):
        - Beijing District 6
    - Alibaba Cloud(including but not limited):
        - Hangzhou Server Room
        - Shanghai Server Room
    - WangsuCloud(including but not limited):
        - Yangzhou Server Room
    - ChinaTelecom e Cloud(including but not limited):
        - Hangzhou
        - Suzhou
        - Guangzhou
        - Beijing
        - Chengdu
    - ChinaMobile Cloud(including but not limited):
        - Hangzhou
        - Guangzhou
        - Beijing
        - Chengdu

- Asia Pacific Region(Including Hong Kong, Macao and Taiwan):
    - Huawei Cloud(including but not limited):
        - Hong Kong
        - Thailand
        - Singapore
    - Amazon Web Services(including but not limited):
        - Tokyo
        - Singapore
        - Hong Kong
        - Mumbai
        - Seoul
        - Sydney
- Europe:
    - Amazon Web Services(including but not limited):
        - Frankfurt
        - Ireland
        - Stockholm
        - Milan

- Paris
- London

- Huawei Cloud(including but not limited):
  - Russia(Collaboration with Sbercloud）

- Africa:
  - Huawei Cloud(including but not limited):
    - South Africa - Johannesburg
  - Amazon Web Services(including but not limited):
    - South Africa - Cape Town

- Americas:
  - Amazon Web Services(including but not limited):
    - Western United States - Northern California
    - Western United States - Oregon
    - Eastern United States - Northern Virginia
    - Eastern United States - Ohio
    - Latin America - Sao Paulo
  - Huawei Cloud(including but not limited):
    - Latin America - Sao Paulo
    - Latin America - San Diego
    - Latin America - Mexico

7.1.2 Security review and inspection

Security incident management: Develop physical security emergency plans with cloud server suppliers, and regularly organize data center employee to conduct security drills. In the event of a physical security incident, the plan will take effect immediately and guide relevant personnel to protect customer assets as much as possible.

7.2 Network security

7.2.1 DDoS protection

BCloud uses DDoS protection from Huawei Cloud, Amazon, Alibaba Cloud and other platforms to protect all data center. automatic detection, scheduling and cleaning ensure stable cloud platform network.

Internal use of abnormal IP self-detection methods to isolate the IP of abnormal

service requests and dynamically block suspicious source addresses.

7.2.2 Anti-invasion protection

- Intrusion detection: Some key server security protection from Huawei Cloud, Amazon and other cloud platforms (Web Firewall WAF and Cloud Firewall CFW).
- Host monitoring: All servers are deployed with self-researched monitoring programs to do real-time monitoring of CPU/memory/bandwidth/disk usage and retain real-time operational data for 3 days; O&M platform can be configured with the following alerts:
  - Resource utilization exceeds preset threshold(CPU/memory/disk/bandwidth for all servers)
  - Bandwidth In/out Difference too large(Mainly used in video streaming servers)
- Database audit: Unified management and strict restriction for database permissions, Complete log auditing of all database additions, deletions and changes; Regular full backup of database at least once a day.

8. Security development management

8.1 Security requirements analysis and product design

In product design stage, Security Technology Center conducts attack surface analysis and threat modeling of system. conduct security review on technologies used in product design, and solved security issues with developers.

8.2 Development stage

In development stage, developers are required to strictly follow security coding specifications, remind developers of security risks in code. After the code is submitted, it is allowed to be merged into the official code branch after strict code review; if there is security problem, notify developers of security fixes.

8.3 Security testing and fixing verification

In product testing stage, for known bugs, security center testers will capture and analyze the data interaction network packets, scann device port, if there are known bugs not repaired, return test and repaired to verify.

9. Security operation and maintenance

BCloud security operation and maintenance platform through unified management, strict access control, monitoring inspection to ensure safety of operation and maintenance.

Account management and identity authentication: use company internal Task account to manage employee accounts, each employee has only a unique account; ensure that only company's active employees can access the O&M platform. Active employees also need authorization by Network Security Center director to access the operation and maintenance platform.

Authorization: Network security center director manages account authorization and sets scope of authority to view or operate operation and maintenance platform.

Monitoring: BCloud uses automated monitoring system to monitor cloud platform network equipment, servers, databases, application clusters, and core businesses in real time. This monitoring system use dashboards to display BCloud key operation indicators, and can configure alarm thresholds. When the key operation indicators exceed the set alarm threshold, Automatic notification maintenance and management employees.

9.1 Customer security service support

Our company's website provides Network Security Segment, including "Security Bulletin" and "Vulnerability Report", and 7x24 customer service hotline.

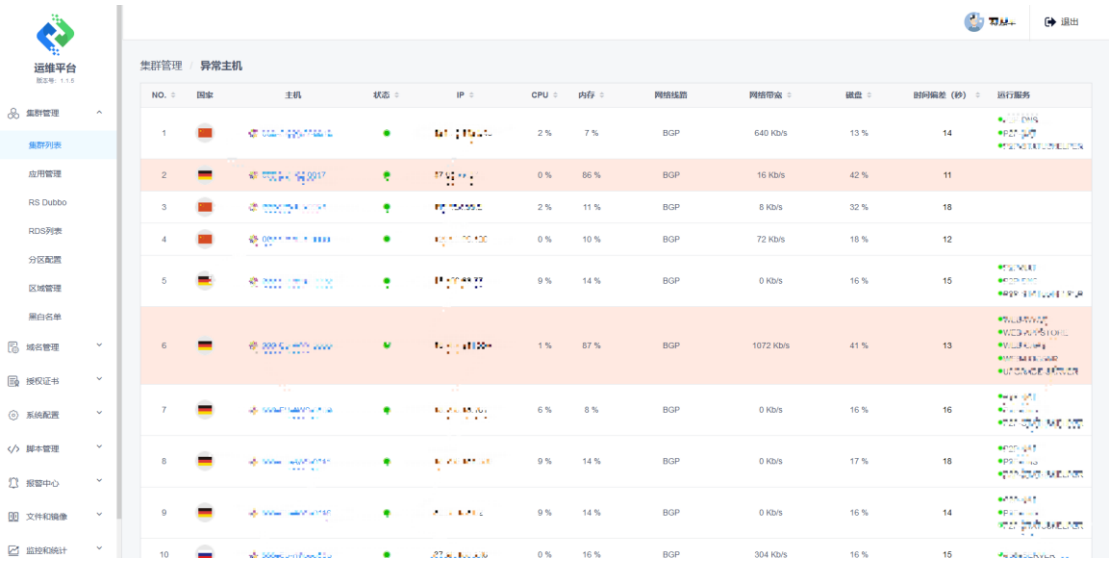
9.2 Maintenance platform warning

operation and maintenance platform duty is divided into two parts: manual duty and robot catches abnormal active warning.

9.2.1 Manual duty

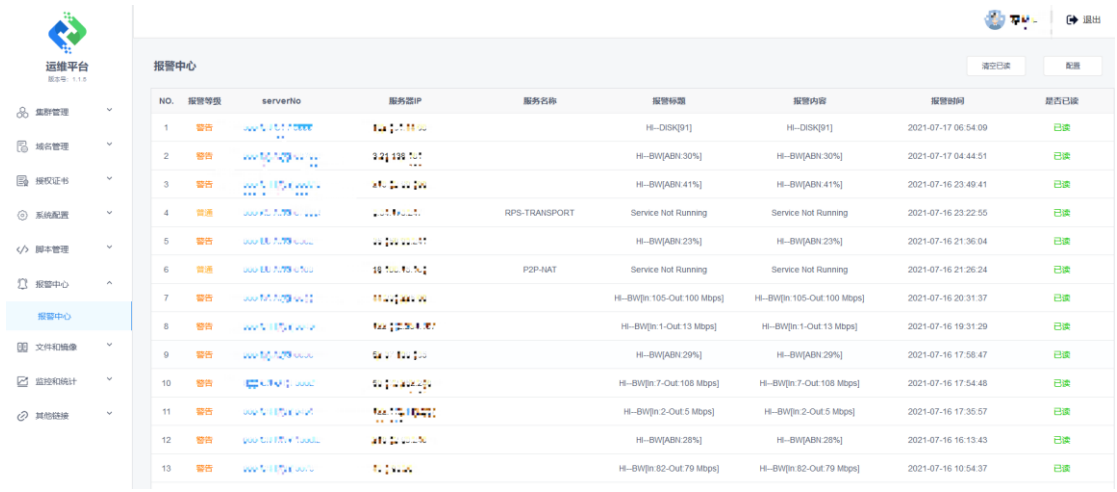
Manual duty employee need to check the "Cloud Platform Operation and Maintenance Daily Checklist (Checklist)" every day to check all business servers in Bcloud; take the initiative to analyze the status of abnormal servers in platform and analyze the causes of abnormalities and failures.

The following chart is the list of abnormal hosts in the operation and maintenance platform, which is analyzed and handled by the duty officer every day:



9.2.2 Robot warning

Operation and maintenance platform automatically analyzes abnormal behavior of cloud host in real time, push alarm notifications to operation and maintenance management employee with DingTalk robot and WeChat service account, and deal with and solve problem in the first time



DingTalk robot and WeChat service account real-time alarm notification:

10. Business security and risk control

10.1 Account security

Account security is the foundation of Jufeng's cloud service system, so strict security control and log audits have been carried out for account registration, login, password retrieval, and multi-device login. At the same time, the data storage, query and modification of the account system are strictly protected. Strict policy protection is carried out against common account risk sources such as database collision and API abuse.

At the same time, the weak password is checked during user registration, and the

setting of common weak passwords is prohibited.

10.2 Content security

All business data has a specific business authorization code. Only when the account login is normal, the business authorization code below will be used. The authorization code is dynamic, and the content submitted by the terminal is verified by data to reduce security risks.

11 Terminal security

11.1 App terminal

All App terminal have a unique AppKey, only applied for the corresponding App key can be allowed usage. When the system detects a malicious request from the App, the platform can terminate all data requests from the App client.

11.1.1 Client program protection

The security of the client itself is often the first hurdle for hackers to break through the security of the APP client. From the hackers side, the attacker needs to get the source code of the client, and then quickly interpret the code, including finding specific keywords or methods, and finding vulnerabilities. Therefore, a threshold needs to be added in this process. In addition, it is also very important to protect the application package from being repackaged. APP client protection includes anti-tampering, code obfuscation, simulator detection and interception, Root environment detection alarm, debugging prevention, interface hijacking protection, hook plug-in detection and process injection protection, etc.

11.1.2 Component safety

For the four major components, Activity, Broadcast Receiver, Service, and Conent Provider, strictly restrict the use and access rights of the components, and perform strict permissions and input verification for externally developed components. For WebView, maintain a higher version of the SDK, and strictly control the URL domain name and file access authority.

11.1.3 Data Security

1. The APP client strictly controls the data stored locally on the client.
2. Internal storage:
   a) Private directory: The configuration files and other information that must be stored in the local part are stored in a secure encryption method. At the same time, the key is unique for each user. At the same time, strict read-write execution authority settings are adopted.
   b) Android's Shared Preferences configuration file: Sensitive information is not allowed.
3. System log: The official client does not print and store any interactive logcat or log files.
4. Key chain data: hard-code important keys. Use self-developed security algorithm to save the key
5. Memory data: During important operations, user data is not stored in the memory.

11.1.4 Communication security

- SSL encryption support, HTTPS support;;
- RSA+AES encryption support for device interaction data;
- Video stream private encryption support;

11.2 Hardware and firmware security

11.2.1 Communication security

According to different CPU main control chips, Jufeng provides different levels of encryption mechanisms to maximize the security protection of the chip. No matter which encryption mechanism is used, data communication security is guaranteed. At present, the NETIP private encryption protocol and HTTPS provide additional AES encryption protection for data and control commands in the interactive process. A device-based, unique random key generated based on encryption algorithms such as MD5 and true random numbers.

At the same time, all communication data of Jufeng will use multiple data protection mechanisms such as anti-replay verification, device identity verification, access control and authorization verification.

11.2.2 Firmware protection

Jufeng implements multiple protection mechanisms for firmware:

1. Firmware flash read and write protection, according to the degree of support of the chip's platform, the read and write of the firmware is restricted to prevent the firmware from being read and written through the hardware, and at the same time to prevent the device system firmware from being maliciously modified;

2. Firmware encryption protection, some platforms support firmware encryption, and Jufeng will enable it;

3. Firmware anti-counterfeiting verification, Jufeng firmware will be signed by Jufeng's certificate;

4. Code obfuscation, additional obfuscation and protection of the core code, especially the encryption module。

11.2.3 OTA Security

1. Trustworthy startup, Jufeng will perform firmware tamper-proof protection according to the capabilities of the chip platform, and verify the startup of the core system or all firmware.

2. Trustworthy upgrade. When the device upgrades the firmware, the upgrade server will perform trusted verification on the firmware and refuse to write illegal or tampered firmware to the device. At the same time, after the device is completely downloaded, the legality and integrity of the entire upgraded firmware are fully verified. After verification, the official upgrade begins;

3. Trusted execution. During the operation of the device, any executable program needs to pass the trusted verification of the kernel before being loaded and run to avoid malicious program execution and intrusion into the device.

11.2.4 Data protection

- User data protection

  Encryption technology is used to protect user data. User data mainly includes user configuration data and user privacy data. Data encryption prevents data fees from being cracked by attackers after they are forcibly copied. User data mainly refers to configuration parameters and usage information, excluding face comparison pictures, models, etc.

- Storage media encryption

  Supports the encryption of various data on various storage media to avoid data leakage, especially the encryption of key data (audio and video data) on pluggable storage media, etc.

- digital water mark
  Digital watermarking is an information hiding technology. Its basic idea is to embed encrypted information in data products such as digital images, audio and video, protect the copyright of digital products, and prove the authenticity and reliability of the products. Digital watermarking provides a way to hide the logo. The logo cannot be seen on the original file. It can only be read by a special reading program. Adding a digital watermark to the video stream can be an ideal way to solve the video tampering attack. It can be judged whether the video information has been tampered with.

11.2.5 Configure network security

The Wi-Fi device found before the network distribution, the broadcast information sent by the APP and hardware are transmitted through AES encryption and so on.

During the network distribution process, APP uses AES encryption to transmit to the hardware WIFI information, which ensures the security of the user's network and reduces the risk of the network distribution process.

12. Business sustainability

12.1 Business continuity

In order to eliminate the interruption of key production and operation activities and avoid the impact of major failures or disasters, all hosts, applications, services, networks, etc. of the cloud platform are monitored in real time through the operation and maintenance platform, and there is a complete set of business failure automation Process system and guarantee, through multi-service hot switching to ensure uninterrupted service.

In view of the risks caused by non-resistance factors such as business system software and hardware failures and even natural disasters, a complete set of response plans has been specified, which is capable of ensuring business continuity under foreseeable conditions.

12.2 Disaster recovery

The real-time hot backup of master-slave data, redundant storage and ground backup are adopted to ensure the safety, reliability and continuous availability of business data. And real-time monitoring and verification of the backup situation. At

the same time, for business systems, multi-link backup systems, to ensure rapid emergency switching.

12.3 Emergency plan

The operation and maintenance team has internally established emergency plans and measures for various types of assets and security risks, which can ensure that emergency treatment can be carried out correctly, orderly, and efficiently after the event, and the normal operation of the work is guaranteed. The emergency plan includes pre-planning procedures, monitoring and a series of failure response methods. Through detailed system monitoring and review records during the event, sufficient information can be provided after the event to be able to quickly understand and analyze, as well as the corresponding interface personnel. After the event, there is a complete set of processing procedures and emergency plans to ensure that problems can be handled quickly, and problems can be analyzed and held accountable.

12.4 Emergency drills

Regularly implement large-scale hardware failures, network DDoS, security incidents and other internal technical emergency drills and tests and actual combat.