



Tuya Smart Information Security White Paper

Version 3.1.201912

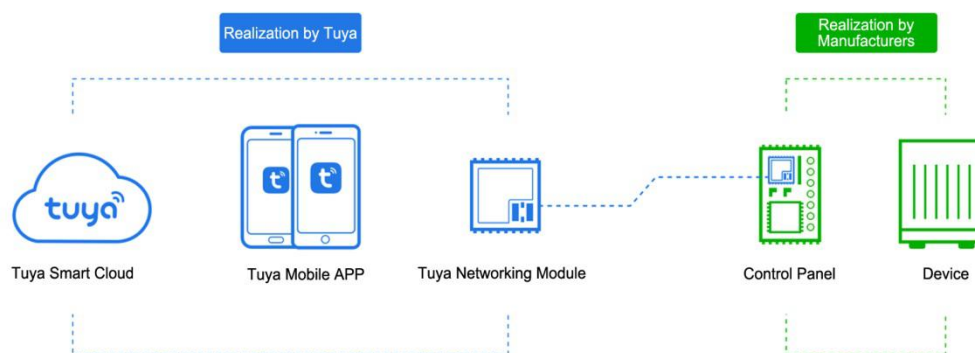
Catalog

1.INTRODUCTION TO TUYA SMART.....	1
1.1 INTRODUCTION TO TUYA CLOUD PLATFORM.....	1
1.2 MISSION ON INFORMATION SECURITY ASSURANCE.....	1
2.SECURITY RESPONSIBILITIES.....	2
2.1 SECURITY RESPONSIBILITIES OF TUYA CLOUD.....	3
2.2 SECURITY RESPONSIBILITIES OF CUSTOMERS.....	3
3. COMPLIANCE ENDEAVOR.....	3
3.1 ISO 9001.....	4
3.2 ISO 27001.....	4
3.3 ISO 27017.....	5
3.4 ISO 27018.....	6
3.5 GDPR.....	6
3.6 CCPA.....	7
3.7 TEST ASSESSMENT OF "INTELLIGENT HARDWARE (IoT) OPEN PLATFORM".....	7
4. DATA SECURITY.....	8
4.1 DATA SECURITY SYSTEM OF TUYA CLOUD.....	8
4.2 DATA PROPERTY.....	8
4.3 MULTI-COPY REDUNDANT STORAGE.....	8
4.4 USER DEVICE DATA SECURITY.....	9
4.5 ENTERPRISE DATA SECURITY.....	10
4.6 ELIMINATION OF RESIDUAL DATA.....	10
4.7 PRIVACY PROTECTION.....	10
4.8 DATA STORAGE AREA.....	11
5.INFRASTRUCTURE OF CLOUD PLATFORM.....	13
5.1 INFRASTRUCTURE DIAGRAM.....	13
5.2 REQUIREMENTS FOR CLOUD SERVER PROVIDERS.....	14
6.SECURITY ORGANIZATION AND STAFF.....	14
6.1 SECURITY AND PRIVACY PROTECTION TEAM.....	14
6.2 HUMAN RESOURCE MANAGEMENT.....	14
6.3 SECURITY AWARENESS AND EDUCATION.....	15
6.4 TRAINING FOR SECURITY MANAGEMENT.....	15
6.5 IMPROVEMENT OF INFORMATION SECURITY CAPABILITY.....	15
7.SECURITY ASSURANCE OF CLOUD PLATFORM.....	15
7.1 PHYSICAL SECURITY.....	15
7.2 NETWORK SECURITY.....	16

8.SECURITY DEVELOPMENT LIFECYCLE MANAGEMENT.....	19
8.1 SECURITY DEMAND ANALYSIS AND PRODUCT DESIGN.....	20
8.2 DEVELOPMENT STAGE.....	21
8.3 SECURITY TEST, FIXING AND VERIFICATION.....	22
9.SECURITY OPERATION AND MAINTENANCE.....	23
9.1 SECURITY RISK MANAGEMENT.....	24
9.2 CUSTOMER SECURITY SERVICE SUPPORT.....	25
10. BUSINESS SECURITY AND RISK CONTROL.....	26
10.1. ACCOUNT SECURITY.....	26
10.2. CONTENT SECURITY.....	26
11. TERMINAL SECURITY.....	26
11.1 APP.....	26
11.2HARDWARE AND FIRMWARE SECURITY.....	27
12 BUSINESS SUSTAINABILITY.....	29
12.1 BUSINESS SUSTAINABILITY.....	29
12.2 DISASTER RECOVERY.....	29
12.3 EMERGENCY PLAN.....	29
12.4 EMERGENCY DRILL.....	30

1. Introduction to Tuya Smart

Tuya provides a leading global IoT platform that enables manufacturers, brands, OEMs and retail chains to develop one-stop smart home solutions. Tuya is internationally operated with headquarters in U.S., Germany, India, Japan and China.



To-date, Tuya has 180,000 clients in over 190 countries who are delivering over 90 thousand Powered by Tuya products, covering 500 types of products, ranking the first in the industry, including lighting, appliances, entertainment and security solutions.

1.1 Introduction to Tuya Cloud Platform

Tuya implements cloud services around the world and devotes itself to providing stable, secure, and fast Tuya Cloud Services. Tuya Cloud has one hundred million massive data and ten million users concurrent processing capacity. It is able to provide uninterrupted service with 99.99% uptime. Through integration of global service nodes in AWS and MS Azure, Tuya Cloud is able to provide access to nearby services for users in different regions of the world to ensure efficient and stable equipment experience, helping China manufacturing services worldwide.

The platform is equipped to provide complete lifecycle services ranging from product definition, simulation testing, hardware development, client development, cloud-to-cloud platform interaction, platform testing, operational management and data analysis of smart products. Tuya Cloud offers makers and vendors self-service software/hardware development SDK, a well-established open cloud platform API and a debugging assistant to lower the development threshold for hardware manufacturers. The platform saves R&D costs and accelerates the process for smart product development for manufacturers. In addition, it helps manufacturers to upgrade software/hardware intelligence and continues to provide premium services for end consumers.

1.2 Mission on Information Security Assurance

Tuya is devoted to providing customers with consistent, reliable, secure and conforming IoT access services, and guaranteeing the availability, confidentiality and integrity of the data of users. Tuya Cloud's promise: Tuya Cloud has data protection at its core and is built on cloud security. It relies on Tuya's unique IoT solutions to establish itself as a competitive leader in the business, develop a complete cloud security system, and make information security consistently one of the key development strategies for Tuya Cloud.

To achieve the objectives, Tuya has realized all-round protection and deployed security protection in all levels, including security check, security defense, security monitoring and audit for all the external services, thus to realize prior, in-process and post-protection.

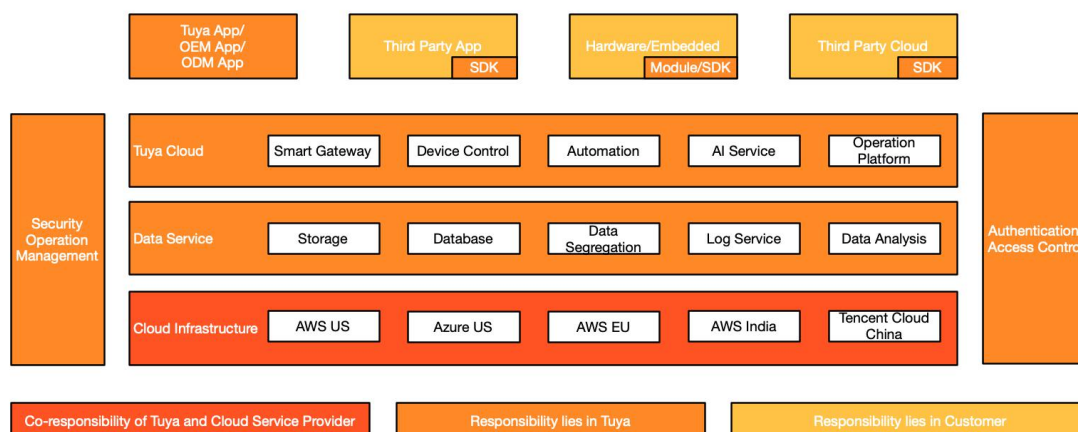
The White Paper will present the security concerns of Tuya Cloud in the following aspects:

1. Security responsibilities
2. Compliance
3. Data security
4. Infrastructure of cloud platform
5. Security organization and personnel
6. Security assurance of cloud platform
7. Security development lifecycle management
8. Security operation and maintenance
9. Business security and risk control
10. Terminal security
11. Business sustainability

The White Paper aims to provide customers with in-depth understanding of Tuya and in-depth security insight of Tuya Cloud.

2. Security Responsibilities

Tuya handles security management and operation for services and data exchange on Tuya Cloud and takes responsibility for security of the cloud service platform and infrastructure. To have embedded software for Apps or hardware developed by clients (including by use of SDK) access to Tuya Cloud, the clients will have to guarantee the application and data (see Article 2.2), including hardware and App security compliance. The diagram below shows how the responsibility of information security is shared among infrastructure cloud service providers, Tuya, and clients.



2.1 Security Responsibilities of Tuya Cloud

Tuya Cloud ensures the security of infrastructure for security management and operation and physical devices by leading cloud hosting provider Amazon and cloud computing platforms MS Azure.

Tuya Cloud covers data security and cloud service security, and Tuya promises to use its security team and the professional experience of external security service providers in intrusion and protection technology to provide security operation and maintenance for Tuya Cloud, practically protect its operation security, and guarantee the security of customer and user privacy and data. This promise mainly includes but is not limited to:

- **Data security:** security management of customers' business data in cloud computing environment, including collection and identification, classification and grading, authority and encryption, as well as the privacy and compliance requirements.
- **Access control management:** resource and data access permission management, including user management, authority management, and identity authentication.
- **Cloud service security:** security management of business-related application system in cloud computing environment, including design, development, release, configuration and use of applications and service interfaces.

2.2 Security Responsibilities of Customers

For Apps developed based on Tuya's SDK, Tuya will only provide technical support, but not any security guarantee. For information on data security compliance and the privacy policy for Tuya-based OEM (public version) Apps (without customized scenarios), Tuya has made templates available to clients. Clients will be responsible for actual privacy policies and compliance statements to be released online. The Tuya security team is available to provide assistance and advice on security solutions if necessary.

3. Compliance Endeavor

Global IoT Presence

Tuya follows international security standards and industry requirements and builds them into the internal control framework. Compliance is strictly enforced in the process of implementing Cloud and App specifications.

- Tuya is a member of the Smart Home Appliance Cloud-Cloud Connectivity Work Group of the China Household Electrical Appliances Association (CHEAA) and
- The leader of the Security Team under the Smart Home Appliance Cloud-To-Cloud Connectivity Work Group. It plays a guiding role in establishing cloud-to-cloud connectivity information security standards for smart appliances in China.
- Tuya also participated in the making of smart home appliance information security standards for the National Intelligent Building and Residential Digitalization Standardization Technical Committee (SAC/TC 426) in China.
- Recently, Tuya plays as the guiding role in the China Communications Standards Association, and participated in the formulation and writing of the IoT documents.

Tuya also cooperates with independent third-party security service providers, consultants and auditors to validate and guarantee the compliance and security of Tuya Cloud.

Tuya has completed information security & privacy and compliance certification/validation with the consultation of various global agencies, and now serves as an IoT solution provider with the most comprehensive certificates in Asia. Tuya is ongoing to, and will audit and the internal security framework and organization with continuous endeavor.

See the following for our certification and compliance certificates. Tuya is continuously working on more Verification and Compliance Certificates on Information Security and Privacy Security.

3.1 ISO 9001

ISO 9001 comes from the first quality management system standard - BS 5750 (prepared by BSI) in the world, and is the most mature quality framework in the world up to now. ISO 9001 serves as a systematic guiding outline and standard framework to ensure the product quality and operation of an organization. It also covers the entire process of planning, implementation, product improvement and realization of services, with products or services provided by the organization as the core, so as to ensure meeting the requirements of customers and those in relevant laws and regulations.

Quality management system can be used to realize expected quality objectives effectively and efficiently, corrective and preventive actions can be taken upon the audit and management review of quality management system to realize continual improvement of the effectiveness of quality management system, which is fundamental for corporate development and growth.

3.2 ISO 27001

Currently, Tuya has obtained ISO 27001 Information Security Management System Certification (ISMS).



ISO 27001, as an international standard of Information Security Management System, provides best practical guidance for the establishment and operation of information security management system for different kinds of organizations. According to the requirements in this standard:

- Tuya establishes, implements, operates, monitors, reviews, maintains and improves information security with the methods based on business risk;
- Tuya has set up a corresponding organization, established systematized security management system, and provided resource guarantee, to ensure information confidentiality, integrity and availability;
- Tuya continuously improves information security management according to PDCA approach.

3.3 ISO 27017

Tuya has obtained ISO 27017 Certification for information security of cloud services.



ISO 27017 gives guidelines for information security of cloud computing, recommends special controls for cloud information security, and makes supplementation to the guidance of ISO 27002 and ISO 27001. This Code of Practice provides cloud service providers with additional implementation guidance for information security controls.

Tuya Smart has greatly promoted the implementation of ISO 27017 certification through months of efforts, which indicates that Tuya Smart adopts international recognized best practice all the time, and also proves that Tuya Cloud is set with special high-accuracy control system for cloud services.

3.4 ISO 27018

Tuya has obtained ISO 27018 Certification for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors. Tuya is committed to compliance of international privacy right and data protection standards.



ISO 27018 is a code of practice for the protection of personal data in the cloud. Based on ISO 27002 Code of Practice for Information Security Controls, ISO 27018 provides the guidance for the implementation of ISO 27002 control system applicable to personal identifiable information (PII) in a public cloud. It also provides a series of other control systems and relevant guidance to meet the requirements for the protection of PII in a public cloud which is not provided in the existing ISO 27002 control system combination.

Tuya has passed SGS expert panel review on compliance of ISO 27017 & 27018 (the two internationally recognized codes of conduct).

3.5 GDPR

The EU General Data Protection Regulation (GDPR) is intended to protect the fundamental privacy right of EU data subjects and the security of personal data. It calls for more rigorous protection standards and requirements and sets a high cost for breach, all of which have significantly raised the security, compliance standards, and costs for businesses in processing and protecting information of EU citizens.



With the partnership with TrustArc, a global Privacy consulting firm, Tuya was completely assessed and verified through TrustArc's systematic and rationalized platform, preparation and development, as well as implementation of a set of comprehensive compliance remediation plans throughout the whole organization. A strong demonstration of fully compliance with the GDPR regulation is the Validation Report officially released by the TrustArc.

3.6 CCPA

The California Consumer Privacy Act (CCPA) is a bill that enhances privacy rights and consumer protection for residents of California, United States. The Act was made public by the California State Legislature on June 28, 2018 and will take effect on January 1, 2020.

By partnering with the TrustArc in further, Tuya exhibits a high level of preparatory and program maturity as regards privacy and security for the enterprise, cloud, IOT and mobile environments, has demonstrated a commitment to compliance efforts and reported favorably in responses about most of the needed programs and preparations currently in place.

3.7 Test Assessment of "Intelligent Hardware (IoT) Open Platform"

According to CAICT test assessment for "Intelligent Hardware (IoT) Open Platform", Tuya Cloud is recognized for platform openness, security, stability, and concurrent performance of platform processing device connection.



4. Data Security

4.1 Data Security System of Tuya Cloud

According to the life cycle of data, the data security system of Tuya Cloud is developed for comprehensive and systematic construction by management and technical means. The data security targets are met by enforcing data security control and management in every stage of the data life cycle (data collection, storage, processing, transmission, sharing, and deletion).



Meanwhile, there is corresponding security management system and security technology guarantee at each stage of the lifecycle of data.

4.2 Data Property

In the customized solution, Tuya only acts as the data processor and the data generated shall be controlled by the respective Customer, namely the data controllers. Data processing activities are followed Customers' written instruction, which shall be documented in the contracts or addendum, on the lawful and transparent basis. Therefore, given compliance with the laws and regulations and the privacy policy, Tuya can help clients and users protect data confidentiality, integrity, and security.

4.3 Multi-copy Redundant Storage

Under the distributed architecture, all servers are deployed simultaneously among three server rooms in different areas of the same city. Databases and other data storage services follow a multiple backup model (keeping a minimum of two real-time copies) that performs real-time backup. The approach guarantees high reliability and high availability of data and services.

4.4 User Device Data Security

Tuya Cloud provides multiple security policies to guarantee the security of the data generated by different smart devices. See the figure below:



In terms of device-cloud interaction:

- Data encryption: AES -128 is adopted for data content encryption.
- Authorization authentication: Tuya's unique algorithm provides multiple guarantees of interactive authentication, access control and effective authorization, such as connection authentication and authorization request, and instruction generation.
- Dynamic key: One device with two codes and dynamic key and dynamic password, to ensure device security.
- Transmission encryption: TLS1.2 data encryption transmission protocol and mutual mandatory authentication.
- Secure chips: Tuya WiFi Modules support using the secure chip versions to have safe storage authorized information and encrypted key, etc.
- Virtual device design: This is to guarantee the devices will still function as well and not affected even the authorized information of devices is stolen, meanwhile, Tuya adopts pseudonymization technology in device id to ensure user privacy and security.
- In terms of interaction between devices in LAN:
- Device isolation.
- Data encryption: AES-128 is adopted for data content encryption before data transmission in LAN.

- Dynamic key: Dynamic distribution of algorithm during network configuration.

For further information regarding the security protection of the devices, please refer to Chapter 11.2.

4.5 Enterprise Data Security

In regards to enterprise data security, Tuya Cloud isolates enterprise data to guarantee data security. Tuya Cloud provides different data storage services for customer and user sensitive data by AES256 in different business scenarios to realize encrypted storage. Certain type of sensitive data will be desensitized as necessary. At the same time, the key will be uniformly managed and distributed through the key management center, KMS.

4.6 Elimination of Residual Data

For any memory and/or disk that was once used for storage of customer data, the residual information will be automatically overwritten with zero upon release and recovery. Any replaced or obsolete storage device will be demagnetized and physically bent in unified manner by the cloud server infrastructure provider before being taken out of data center.

4.7 Privacy Protection

Tuya Cloud adheres to "all based on user value" as the operation principle, and in particular attaches importance to the permanent trust relationship with customers. Tuya ensures complete guarantee for the data of users and customers by solid technical foundation and complete operation management mechanism. Tuya Cloud will protect user privacy in strict accordance with the Privacy Policy in public by Tuya.

Means of Privacy Protection

The major protection means of the Tuya IoT Platform for private data includes:

- Production and Classification of Privacy Data
 - Fundamental Principles:
 - ◆ The principle of lawfulness, fairness and transparency requires Tuya processed lawfully, fairly and in a transparent manner in relation to individuals. All actions of the information collection, including authorization of information and the confirmation of legal liabilities, shall abide by laws and regulations.
 - ◆ Apply the minimum data collection principles, adequate, relevant and limited to what is necessary in relation to the purposes for which Tuya will process and do not collect data that is irrelevant to the services provided.
 - The full right to be informed
 - ◆ Privacy Policy of App and Website
 - ❖ User data types collected by the App and the services provided by using the collected data must be included in the privacy policy.

- ❖ Users must be informed of the privacy policies by email or in App at time of registration, when updated and other key points in time.
- ❖ The privacy policies must include data disclosure, deletion, transmission, storage and user options, etc.
- ❖ Users must be given the option to give feedback on the privacy policies.
- ◆ Statement on Cookies of Website
- ◆ Use of cookies and user options.
- User's Rights:
 - ◆ Right of Access
 - ❖ Users can access personal data collected by Tuya through the App without additional technical support.
 - ❖ Users can make a request to Tuya for any data utility and processing activities associated for his/her personal data.
 - ◆ Right to be Forgotten (Right to Delete Data)
 - ❖ Permission to deregister an account and delete data
 - ◆ Right to Correct
 - ❖ It is applicable for personal information willingly provided by users. In case of inaccuracy, user may modify information manually on the App or contact Tuya to make a correction.
 - ◆ Right to Data Portability
 - ❖ The user can request via App service center or email box for feedback or receive their personal data which they provided to Tuya.
- Data classification.
 - ◆ The data includes personal data and platform data, which we called general data. For personal data, encryption of the sensitive data shall be adopted.

4.8 Data Storage Area

Five data centers, China Server Room, US Server Room in AWS, US Server Room in Azure, and European Server Room and India Server Room (with data centers physically isolated from each other and not connected), providing data services according to user's location. More server rooms will be made available in the future.

- China: The data is stored in BGP server room in Hangzhou, China, and basic cloud computing support is provided by Aliyun.
- America: The data is stored in a server center in Oregon or Virginia, U.S.A., and basic cloud computing support is provided by Amazon AWS by default or Microsoft Azure that customer can choose for.
- European Union: The data is stored in a server center in Frankfurt, Germany, and

basic cloud computing support is provided by Amazon AWS.

- India: The data is stored in a server center in Mumbai, India, and basic cloud computing support is provided by Amazon AWS.
- Other countries: The data is stored in a server center depending on the proximity to Oregon or Frankfurt.

With more regional server centers are being constructed, more regional data center facilities are coming soon.

5. Infrastructure of Cloud Platform

5.1 Infrastructure Diagram



The infrastructure of Tuya Cloud is provided by Amazon and Microsoft, and is integrated with global service nodes. In terms of platform definition, Tuya Cloud provides the service capability with life-cycle coverage from smart hardware access to operation, including product definition, simulation test, hardware development, client development, cloud platform interaction, product testing, operation management, and data analysis. In terms of service, this platform provides makers and manufacturers with self-service software & hardware development SDKs as well as open and improving cloud platform APIs.

See <https://docs.tuya.com/en/cloudapi/> for the details of cloud platform access development documents.

5.2 Requirements for Cloud Server Providers

Tuya Cloud has done due diligence in selecting the most secure cloud server providers in the world, the merits can be counted for AWS and MS Azure:

- The global leading technical giant for Cloud service;
- Secure and stable cloud computing products;
- The most complete global information security compliance, laws and qualifications.

6. Security Organization and Staff

To enhance the security awareness of all the employees and to guarantee customer interests as well as product and service reputation, Tuya Smart advocates "Everyone shall have security awareness" as the common concept and a best practice in the company to cultivate the security culture amongst employees anywhere in the world and at all times. This culture is embodied throughout every HR activity of Tuya, including recruitment, employment, job training, continual training, internal position transfer and resignation. Every employee of Tuya actively participates in the establishment and maintenance of the security of Tuya products and services and carries out security activities as specified in company rules.

6.1 Security and Privacy Protection Team

Tuya has an in-house security technology team, which is composed of the former members from Alibaba, AntFinancial, Baidu and other Internet companies, conventional security manufacturers, including NSFocus and Venus Tech and DAS-Security. For the formulation of compliance team, we have member of privacy officer, who experienced in the data privacy and was served State Street before, a US financial service company. Meanwhile, Tuya invited other professionals and external professional privacy and security consultancies to the subject matter to ensure the security & compliance ecology.

The team as a whole, ensures that the architecture of security and compliance is under controlled, and reliable at each granular perspective.

Internally, Tuya established the Security and Compliance Committee to adhere to regulatory and compliance requirements, supporting as the interpreter of laws and regulations, as well as risk and compliance enforcement for Tuya as a whole, including Operation and Business Stakeholders.

6.2 Human Resource Management

The human resource management framework of Tuya is consistent with global human resource management framework of the company, and both the frameworks are established on the basis of laws. The role of security for HR sector mainly includes ensuring that employee background and qualifications meet business requirements of

Tuya. All the employees act according to the requirements of all the laws, policies, processes and code of commercial behaviors of Tuya. All the employees have necessary knowledge, skills and experience to fulfill their duties.

Any turnover on the employees' end, strict automatic and human labored measures are performed to revoke and retrieve all electronic devices, servers, accounts of all kinds, and other resources related to guarantee the safety issues.

6.3 Security Awareness and Education

To enhance the network security awareness of all the employees, avoid network security violation risk, and ensure normal business operation, Tuya has released Information Security Manual for Employees of Tuya Smart, based on which employee education of network security awareness is held regularly, and all the employees are required to study network security knowledge continuously to understand the policies and systems in the manual, keep in mind what activities are acceptable or unacceptable, be aware of taking responsibility of their activities even without subjective intention, and make the commitment to behaving as required.

6.4 Training for Security Management

In order to enable the company staff to fully comprehend Tuya's information security management policies and effectively promote and implement security policies, Tuya security team and the internal audit team deliver trainings with regards to the data privacy protection, ISO series and Graded Information Security protection, on quarter basis.

6.5 Improvement of Information Security Capability

Tuya holds internal security development training and information security communication regularly, to improve the security skills of employees, to ensure employees are capable of delivering secure and compliant products, solutions and services.

7. Security Assurance of Cloud Platform

7.1 Physical Security

As an IoT cloud computing service provider, Tuya Cloud makes efforts to provide each customer with secure, stable, sustainable and reliable physical infrastructure. Tuya Cloud has established an all-round security management system according to the national standards and supervision requirements related to data center to cover the process from system and policy to process management and follows strict supervision and audits to ensure physical and environmental security of data center of the cloud platform through continuous improvement.

7.1.1 High-availability Infrastructure

Tuya Cloud builds global service nodes through the integration of cloud hosting service providers – Amazon AWS, Microsoft Azure and Tencent Cloud, to provide customers with

secure, stable, sustainable and reliable physical infrastructure.



Tuya Cloud has deployed 5 available regions with coverage of China, Europe, the eastern US, the western US and India according to domestic and overseas marketing regions of Chinese enterprises and in combination with submarine optical cable distribution and measurement in cities in the world.

It includes but are not limited to the western US Oregon main server room and eastern Virginia server room; Frankfurt server room in Europe; server rooms in Tencent Shanghai; and other server rooms in Hong Kong, Singapore, Mumbai, Tokyo, and São Paulo (where space available can be expanded dynamically in response to a corporate user's location).

Tuya Cloud deploys data and systems flexibly in different data centers or different regions to meet disaster recovery requirements for businesses.

7.1.2 Security Check and Audit

Security event management: physical security emergency plan is developed with the platforms of the cloud server providers, and the operators at data center are organized regularly for security drill. In case of a physical security event, the plan will be carried out immediately to guide relevant personnel to protect customer's assets to the greatest extent.

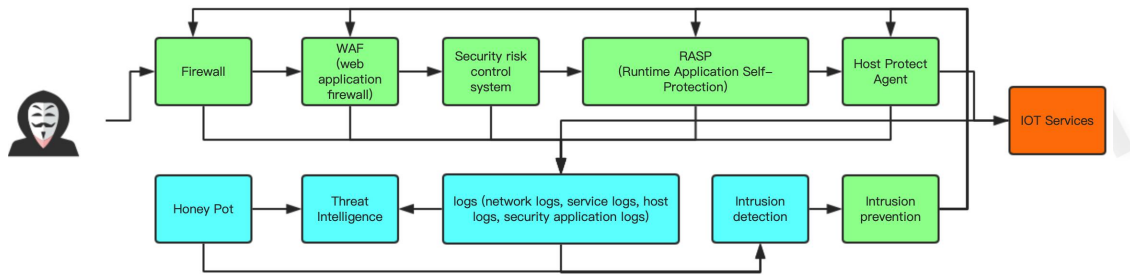
7.2 Network Security

7.2.1 Security Architecture

Tuya Cloud has mature network security architecture, including firewall, WEB Application firewall, Intrusion detection and prevention, RASP (Runtime Application self-protection), host computer protection system and multiple protection mechanisms

against the threats from the Internet.

The network architecture of Tuya Cloud is as shown in the figure below:



7.2.2 Network Communication Security

All communications on Tuya Cloud are encrypted with the TLS security protocol and encryption protection with mandatory certificate authentication, including the communication between Device and Cloud, the API interface is also equipped with a full range of TLS and other security capabilities to enable endpoint security. In the meantime, the AES 128 is applied to its content, two-layer encryption ensures the communication channel.

7.2.3 Network Isolation and Access Control

Tuya has established strict internal network isolation rules to realize access control and boundary protection for internal office network, development network, test network and production network through physical and logic isolation; Tuya Cloud ensures that unauthorized personnel will be prohibited from access to any internal network resource; and all the employees need to pass strict approval and permission control by the Jumpserver before logging in part of the production system and develop routine operation & maintenance, with the entire process being audited.

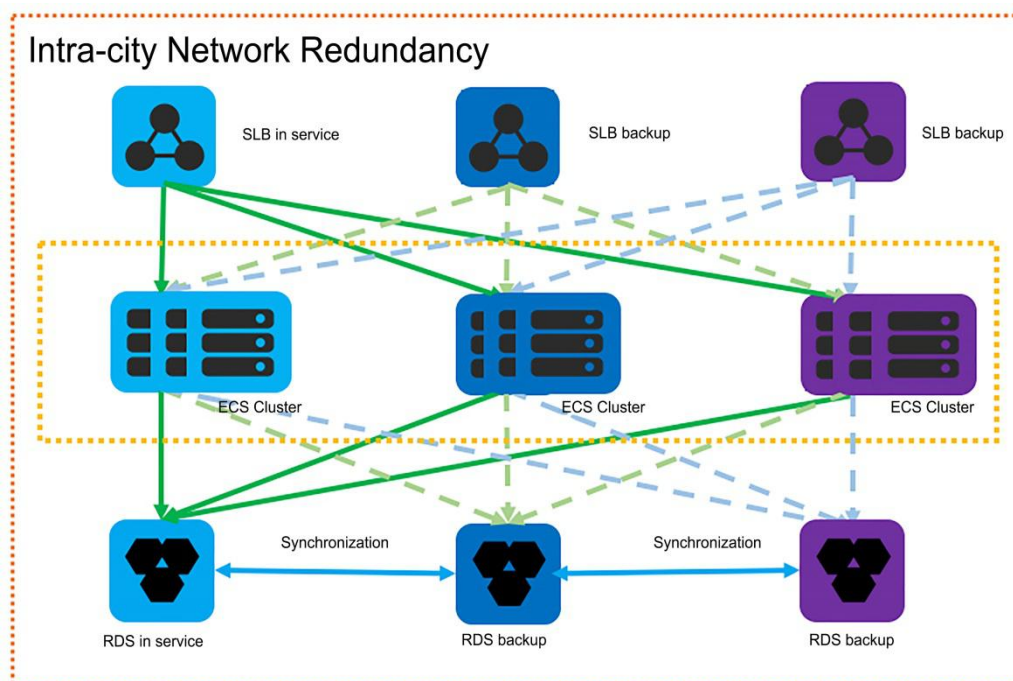
In regards to the network access isolation for cloud users, Tuya provides multiple security mechanisms including virtual-control-level resource access control policy, inter-private network isolation policy in cloud platform, Web console permission distribution and authentication, interface conversation ID and access key, thus to ensure that customers can only have the access to the relevant data generated by their users, and realize access isolation among customers effectively.

7.2.4 Network Redundancy

Data service cloud hosts of Tuya Cloud are distributed all over the world to create cross-region disaster recovery capability for the network and minimize the business impact due to network faults caused by non-human factors.

Redundant network structure has been adopted, with multiple physical Data Center Facilities deployed in the same city to realize convenient network and engineering dispatching of traffic load, prevent network service from interruption due to single-point fault, and realize local and inter-city disaster recovery.

See the figure below for multi-server-room network redundancy deployment in a city:



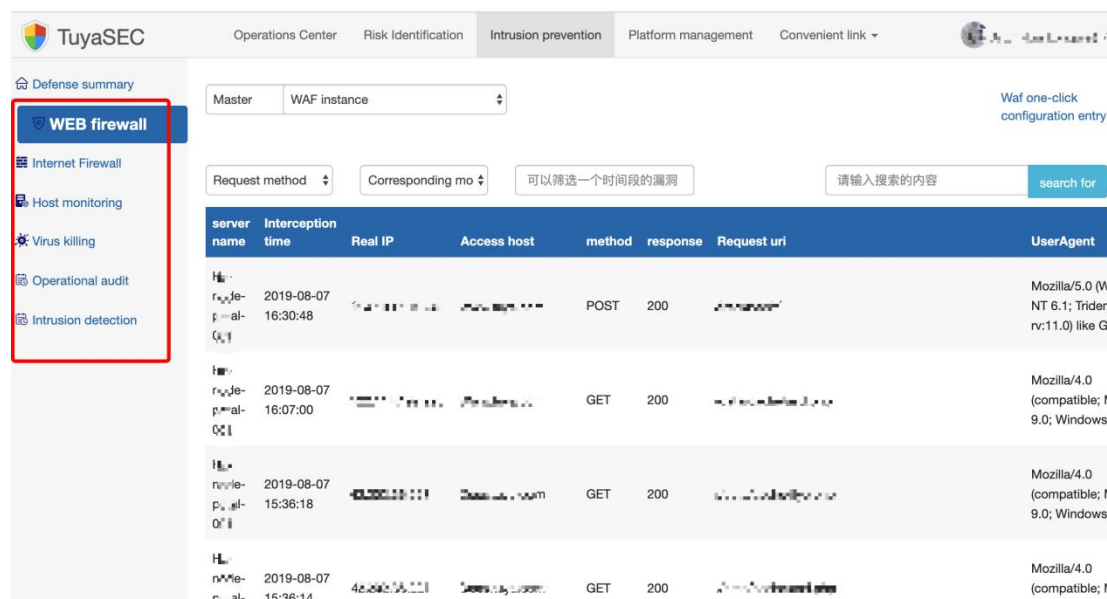
7.2.5 DDoS Protection

Tuya Cloud adopts DDoS protection function of AWS and Azure to protect all the data centers; automatic detection, dispatching and cleaning are performed within not more than 5s response time from attack to cleaning, thus to ensure the stability of cloud platform network.

Use WAF to prevent the CC attack. Check all abnormal IP address by analyzing all request logs and threat intelligence data of third parties and dynamically shield suspicious source address.

7.2.6 Intrusion Prevention

- Intrusion detection: real-time log audit and security analysis are performed for all the servers, applications and networks to quickly detect security risks and notify security team. Invoke the threat intelligence interfaces of third parties. The firewall and WAF will be used automatically to stop threats in case threats, such as abnormal IP address, domain name address, etc., are detected.

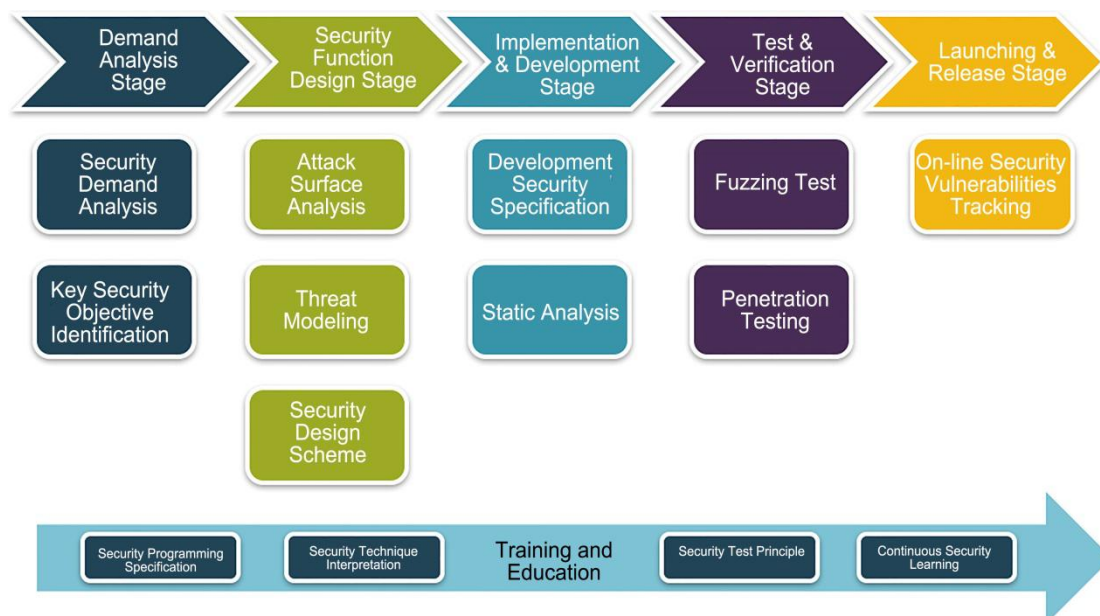


- Intrusion prevention: intrusion is blocked by firewall and WAF.
- Host computer supervision: including WEBSHELL detection, under which servers are provided with webshell real-time detection engine to enable real-time detection, deletion and reporting to webshell; and host computer abnormal login detection, insecure baseline configuration detection, host computer vulnerability detection etc.
- Database audit: strict unified management and restriction are performed for database permission, and complete log audit is performed for all the entry additions, deletions, modifications and inquiries of database.
- Virus inspection: Regular check the file storage server for file security, virus inspection, or executable files.

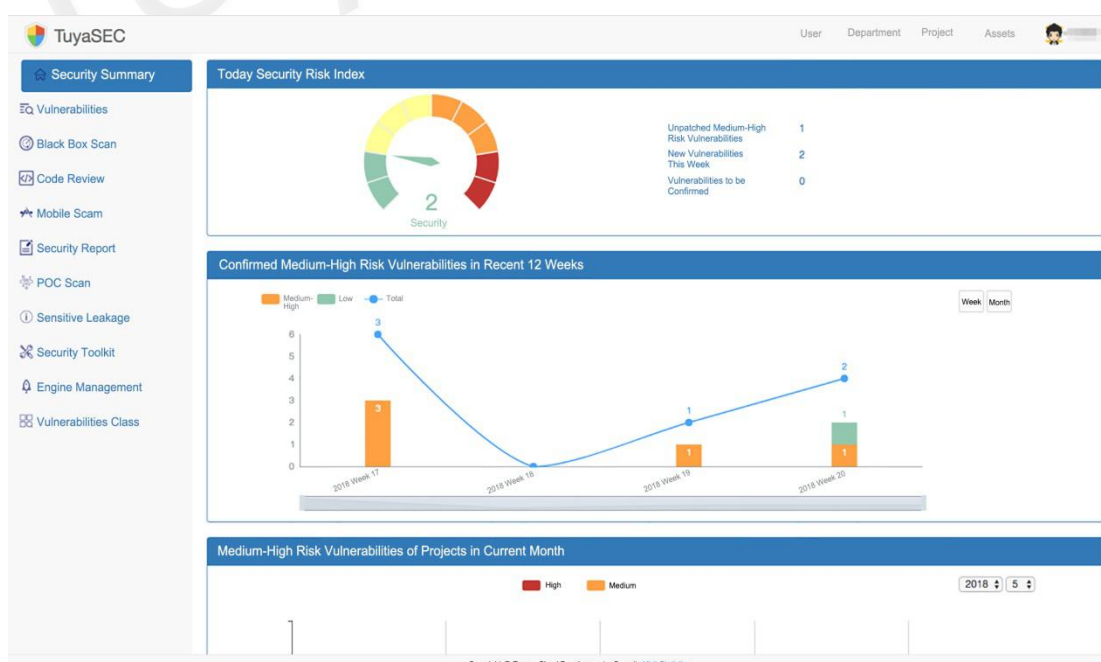
8. Security Development Lifecycle Management

The cloud platform and the cloud products are developed in strict accordance with the security development lifecycle method, for the purpose of integrating the information security into the whole lifecycle of software development.

Tuya's security development lifecycle fully covers all stages of the system development lifecycle.



Unified project SDL implementation monitoring and management is carried out through the security management platform; and the fully automated process trace and the automatic security rating are substantially achieved.



8.1 Security Demand Analysis and Product Design

During the demand analysis, Tuya's security team will analyze the security demands based on the functional requirement document, create communications regarding the business content, the business process and the technical framework to form the Security Demand Analysis Proposal, and reach a consensus with the business side and the developer regarding such proposal.

During the product design, Tuya's security team will analyze the system attack surface,

establish a threat model, analyze the security of technologies to be used in the product design to form the Product Design Security Proposal, and reach a consensus with the developer regarding such security proposal.

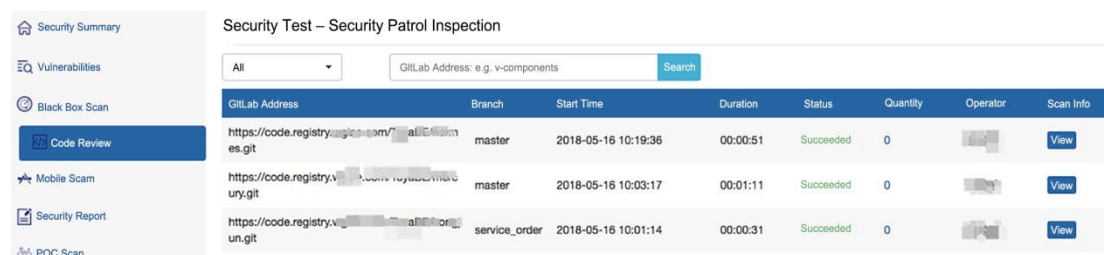
8.2 Development Stage

8.2.1 Safe Development Standards

During the coding phase, Tuya's security team will design a safe development framework for the developer, and require the developer to strictly follow the secure coding standard, provide automatic security IDE plugins, and remind the developer of the security risks during the coding. Meanwhile, upon completion of each code submission, automated code audit will be carried out, and corresponding developer will be noticed to do safe recovery.

8.2.2 Code Auditing

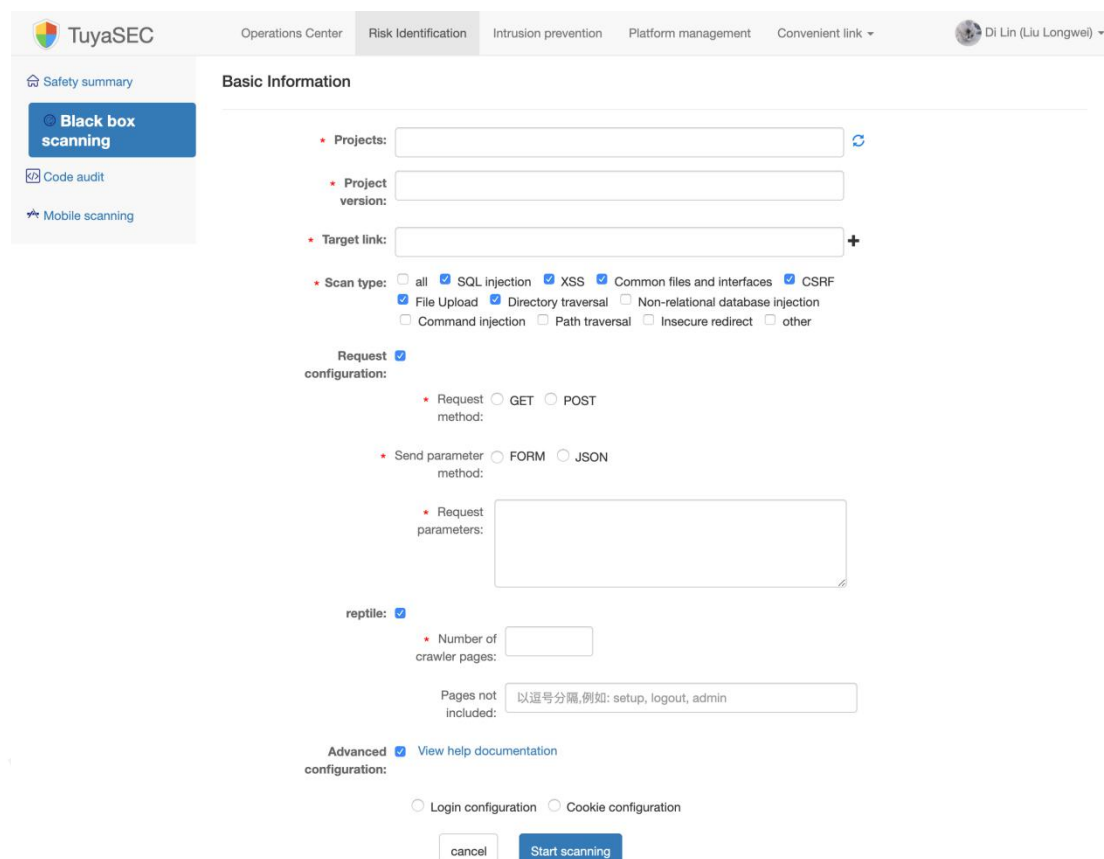
The code audit independently developed by Tuya is able to accurately locate the high-risk function entry by means of the syntax tree analysis, and do retrograde analysis before use of the function, in order to discover the unsecure uses. Meanwhile, prevailing vulnerability information will be tracked in an automated real-time manner, any third-party component library that is considered unsecure will be automatically updated, and rules will be generated for a vulnerability warning.



GitLab Address	Branch	Start Time	Duration	Status	Quantity	Operator	Scan Info
https://code.registry.tuya.com/.../es.git	master	2018-05-16 10:19:36	00:00:51	Succeeded	0		View
https://code.registry.tuya.com/.../un.git	master	2018-05-16 10:03:17	00:01:11	Succeeded	0		View
https://code.registry.tuya.com/.../un.git	service_order	2018-05-16 10:01:14	00:00:31	Succeeded	0		View

8.2.3 Vulnerability Scanner

Tuya uses a passive scanning proxy server. As long as the proxy is activated and tested, the black box scanner can automatically get the project interface (port) for automated security auditing.



TuyaSEC Operations Center Risk Identification Intrusion prevention Platform management Convenient link Di Lin (Liu Longwei)

Safety summary

- Black box scanning
- Code audit
- Mobile scanning

Basic Information

Projects: [input field] ↻

Project version: [input field]

Target link: [input field] +

Scan type:
 ☐ all
 ☒ SQL injection
 ☒ XSS
 ☒ Common files and interfaces
 ☒ CSRF
 ☒ File Upload
 ☒ Directory traversal
 ☐ Non-relational database injection
 ☐ Command injection
 ☐ Path traversal
 ☐ Insecure redirect
 ☐ other

Request configuration:
 ☒ Request method: ☐ GET ☐ POST
 ☒ Send parameter method: ☐ FORM ☐ JSON
 Request parameters: [input field]

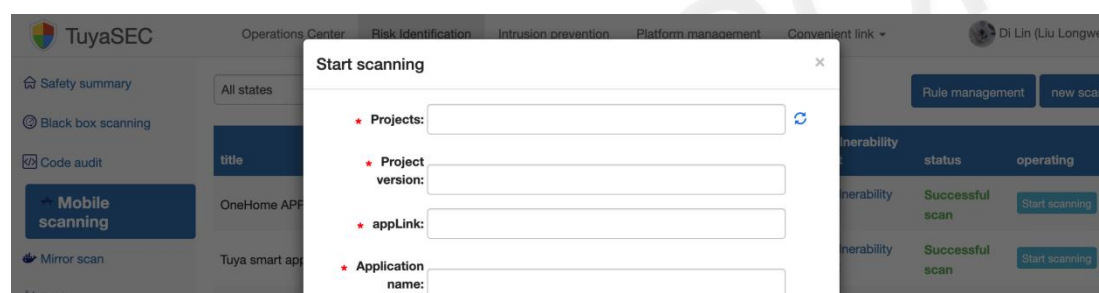
reptile: ☒
 Number of crawler pages: [input field]
 Pages not included: [input field] (以逗号分隔,例如: setup, logout, admin)

Advanced configuration: ☒ View help documentation
 ☐ Login configuration
 ☐ Cookie configuration

cancel Start scanning

8.2.4 Mobile Scanner

Tuya App packaging platform, after completing the new app package, Tuya will automatically send the app package to the mobile scanning platform for scanning, which supports both Android and IOS apps.



TuyaSEC Operations Center Risk Identification Intrusion prevention Platform management Convenient link Di Lin (Liu Longwei)

Safety summary

- Black box scanning
- Code audit
- Mobile scanning
- Mirror scan

Mobile scanning

Start scanning

Projects: [input field] ↻

Project version: [input field]

appLink: [input field]

Application name: [input field]

Rule management new scan

vulnerability	status	operating
nerability	Successful scan	Start scanning
nerability	Successful scan	Start scanning

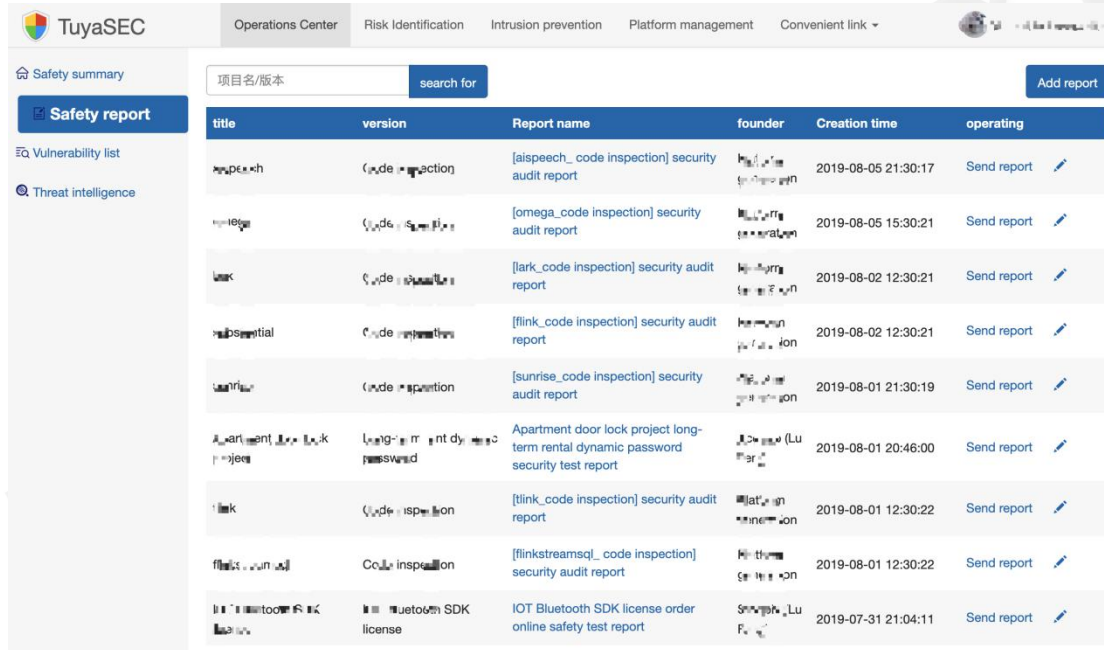
8.3 Security Test, Fixing and Verification

8.3.1 Penetration Test

During the test phase, Tuya's security team will carry out security penetration to discover vulnerabilities by means of the vulnerability scanning platform and the code audit platform in combination with manual tests. If any vulnerability is found, it will be fixed and specifically tracked through the work order system.

8.3.2 Security Vulnerability and Security Test Report

For the release phase, a system can only be released to the online environment after it passes the security test and acquires the Security Test Report, in order to prevent the product from running in the production environment with security vulnerability; the whole system will be reinforced as per the safe online specification during the release process.



title	version	Report name	founder	Creation time	operating
语音识别	语音识别	[aispeech_code inspection] security audit report	语音识别	2019-08-05 21:30:17	Send report
语音识别	语音识别	[omega_code inspection] security audit report	语音识别	2019-08-05 15:30:21	Send report
语音识别	语音识别	[lark_code inspection] security audit report	语音识别	2019-08-02 12:30:21	Send report
语音识别	语音识别	[flink_code inspection] security audit report	语音识别	2019-08-02 12:30:21	Send report
语音识别	语音识别	[sunrise_code inspection] security audit report	语音识别	2019-08-01 21:30:19	Send report
公寓门锁项目长期租赁动态密码安全测试报告	公寓门锁项目长期租赁动态密码	Apartment door lock project long-term rental dynamic password security test report	公寓门锁 (Lu)	2019-08-01 20:46:00	Send report
语音识别	语音识别	[flink_code inspection] security audit report	语音识别	2019-08-01 12:30:22	Send report
语音识别	语音识别	[flinkstreamsqli_code inspection] security audit report	语音识别	2019-08-01 12:30:22	Send report
语音识别	语音识别	IOT Bluetooth SDK license order online safety test report	语音识别	2019-07-31 21:04:11	Send report

9. Security Operation and Maintenance

Unified management is carried out through Tuya's security operation & management platform; and strict access control and monitoring audit are implemented to ensure the O&M security.

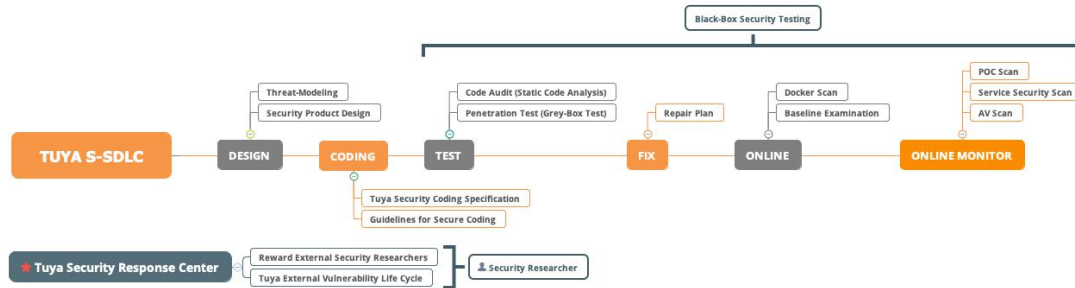
- Account management and identity authentication: every employee account, which is unique to every employee, is managed with a unified account management and identity authentication system throughout the whole lifecycle; the password strategy is issued in a centralized way, and the password strength is constrained; meanwhile, the employees are required to change their own passwords regularly; while Tuya Internal app needs to be installed to receive dynamic verification code for multiple verification method to login.
- Authorization: based on the position and role, Tuya's employees are granted the limited resource access rights as per the principle of the least privilege and the separation of duties. The employees may apply for various access rights from the centralized authorization management platform according to their work needs; and authorization shall be granted upon approvals of the supervisor in charge, the data or system owner, the security manager and relevant departments.
- Monitoring: Tuya Cloud employs an automated monitoring system for comprehensive real-time monitoring of the cloud platform network equipment, the server, the database, the application cluster and the core businesses. The monitoring system

extensively uses dashboard to display Tuya Cloud key operation indicators; and alarm thresholds can be provided to automatically inform the O&M and the management personnel when any key operation indicator exceeds such alarm threshold.

- Audit: all O&M works made to the production system by employees must be and can only be done through the Jumpserver. All operation processes are completely recorded and transmitted in real-time to the centralized log platform. Audit rules are defined for violations; when a violation is found, the security officer will be informed to follow up.

9.1 Security Risk Management

Tuya has an in-house security team taking charge of vulnerability management and discovery, which is able to discover, track, trace and fix security vulnerabilities.



Tuya's security team conducts security penetration tests before any business code is online; meanwhile, and periodically conducts black-box testing for online business.

Each year Tuya also cooperates with third-party security organizations to complete penetration testing on cloud services, mobile clients, hardware products, and even throughout the company products as a whole.

Tuya supports the submission of vulnerabilities by external white hats through channels such like e-mail; Tuya will disclose the vulnerability audit or report results provided by third-party security service company, classify them, rank their severities, track and fix them through work orders.

The vulnerability scores are comprehensively rated in accordance with the technical requirements of attack, the range of affection, the complexity in discovering and using the vulnerability, the importance degree of corresponding business, and the possible damage of the vulnerability as specified in the Tuya's Vulnerability Risk Rating.

Risk Level	Time to Confirm (by Security Team)	Time to Fix (by Development Team)

Emergent	Within 6 hrs.	Within 12 hrs.
High Risk	Within 24 hrs.	Within 48 hrs.
Medium Risk	Within 3 days.	Within 7 days.
Low Risk	Conduct regular Fix Assessment according to the business situations.	

9.1.1 Security Scan

Perform a full network security scan every month, including WEB site vulnerability scanning, application and service vulnerability scanning, host vulnerability scanning, code component vulnerability scanning, and so on.

9.1.2 Third-party security penetration

Third-party penetration testing at least 2-3 times a year. This service is provided by the most professional third-party organizations in the world. The current cooperation organizations include NCC Group, Kaspersky Lab, Vtrust etc. Third-party organizations conduct a comprehensive security assessment of Tuya cloud platforms, apps, and hardware products.

9.1.3 Security incident response

Tuya Incident Response Plan is documented to provide a well-defined, organized approach for handling any potential threat to servers and data, as well as taking appropriate action when the data breach of the personal information. The Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

Tuya also provides survey reports to customers when it affects the stability and security of the customer's business.

9.2 Customer Security Service Support

The complete operation security capability of Tuya Cloud is able to provide customers with 24x7 technical support on cloud services.

10. Business Security and Risk Control

10.1. Account Security

Account security is the foundation of Tuya Cloud service system; therefore, account register, login, password retrieval, multi-device login and the like are all subject to strict security control and log audit. The data storage, query and modification regarding the account system are under strict protection. Common account risk sources like the library hitting and the abuse of API are under strict strategy protection.

Currently, all login and reset passwords and other login-related interfaces use non-marking or sliding verification codes to ensure the ability of man-machine identification ability, preventing malicious registration, collision and other suspicious attacking behaviors.

10.2. Content Security

Dedicated business file type identification and virus scanning, and Trojan scanning engine can quickly identify the security risks of uploaded files.

11. Terminal Security

11.1 App

11.1.1 Client Program Protection

The security of the client is usually the first hurdle for hackers to breach the App client. From the thoughts of black box, the attacker has to acquire the source code of the client and then quickly interpret the code, including looking up the featured keywords or approaches, etc., in order to find out the vulnerability. Therefore, a hurdle needs to be added to this process. In addition, protecting the application package from being packaged again is also an important measure.

Tuya Smart has done a lot of work regarding the App client protection, including anti-tampering in clients, code obfuscation, simulator detection intrusion, building the Root environment detection alarm, prevention of debugging, page anti-hijack technology, Hook detection, and process injection protection.

11.1.2 Component Security

As to the four major components, Activity, Broadcast Receiver, Service, Content Provider, the use and access rights thereof are strictly restricted; and outsourced components are subject to strict permission and input verification.

The latest version of Tuya's SDK is always kept for WebView; and url domain names and file access rights are strictly controlled.

11.1.3 Data Security

Tuya's App client strictly controls the data locally stored at the client.

1. Internal storage:
 - a) Private directory: information such as configuration files has to be stored locally, and saved in a secure encrypted approach, which abides strict read/write settings.
 - b) SQLite database: it does not store user-related sensitive information.
 - c) SharedPreferences configuration file of Android: no sensitive information is allowed.
2. System log: no interactive logcat or log file can be printed or saved at any formal client.
3. Secrete key chain data: important Key cannot be hard coded, and save the key with a self-developed security algorithm.
4. Memory data: user data will not be saved in the memory during important operation.

11.1.4 Communication Security

1. Whole chain channel TLS encryption, including HTTPS and MQTT over TLS and other agreements, compulsory https bi-directional authentication. Server and client certificate information is strictly verified, in order to avoid the risk of being hijacked.
2. The contents of transmitted data and key fields are AES-128 encrypted, simultaneously, the encrypted key is a unique dynamic key generated based on operation of each user.

11.2 Hardware and Firmware Security

11.2.1 Communication Security

According to the performance of different hardware chips, Tuya provides different levels of encryption mechanisms to maximize the chip's security capabilities, all encryption mechanisms ensure the security of data communication. At present, the main communication protocols of Tuya module are MQTT over TLS and HTTPS. Both use TLS1.2 and AES for double encryption protection. and additional AES encryption protection is provided for data and control instructions. TLS uses mandatory verification of identity and certificates, and AES encryption keys use dynamically generated device-based, unique random keys.

At the same time, all communication data of Tuya modules use multiple data protection mechanisms such as anti-replay check, device identity check, access control and permission check.

11.2.2 Firmware protection

Tuya has multiple protections for firmware:

1. Firmware read-write protection, according to the chip's support capabilities, to control firmware read-write entry, preventing firmware reading and writing by hardware.
2. Firmware encryption protection. If the chip supports firmware encryption, Tuya will enable firmware encryption, and Tuya uses a self-developed firmware encryption mechanism to protect the core code.
3. Safe startup, Tuya will perform firmware tamper protection based on the capabilities of the chip platform, and supports startup verification of core code or all code.
4. Firmware anti-counterfeiting verification, Tuya firmware will be signed by Tuya's certificate, and Tuya cloud platform also provides Tuya firmware anti-counterfeiting detection service.
5. Code obfuscation, additional obfuscation and protection for core code.

11.2.3 OTA Security

Tuya supports two methods for firmware upgrade: full firmware update and differential update. Tuya provides multiple protection methods to protect the firmware upgrade process:

1. When generating a firmware package, the packaging tool generates a firmware integrity check message that consists of multiple variables.
2. When the client requests the firmware, the server sends a firmware download information and firmware verification information. The firmware verification information uses a secure HMAC signature algorithm, and the device's unique identity key information is added as a factor to ensure that the firmware cannot be tampered during transmission.
3. After the client obtains the firmware, it needs to calculate the firmware verification information and compare it with the firmware verification information provided by the server. At the same time, it needs to verify the integrity verification information calculated by the packaging tool in the firmware when decompressing. Writing firmware is only allowed after the firmware double check is completed.
4. If the firmware fails to write, or cannot be used normally after writing, it will automatically restore to the original firmware.

11.2.4 Hardware Sensitive Data Protection

Tuya networking module provides support for security chips to store authorization information and encryption keys for networked modules. The authorization information is used to ensure the security and legality of communication between the module and the cloud, and can effectively prevent the authorized data and the encryption key from being stolen or tampered with illegally. The security chip has a secure data area inside. During usage, the Tuya module reads the encrypted sensitive information into the RAM, and if

power down, the sensitive information will loss. At the same time, when the module communicates with the security chip, there will be encryption protection for the temporary key.

For the non-secure chip version, in order to ensure the security of the core data, the important information stored locally will be stored after AES encryption. The encrypted key is randomly generated when each chip is initialized and stored securely. It is only used for local encryption and is not used for any business processing or any interaction.

11.2.5 Pairing Security

The device detection before the pairing, the broadcast information sent by the App and the hardware, and will be transmitted by AES encryption.

During the pairing process, the App uses AES encryption to transmit information to hardware WIFI information, which ensures the security of the user network and reduces the risk of the process.

12 Business Sustainability

12.1 Business Sustainability

To eliminate the interruption to key production and operation activities, and protect them from the impact of major failure or disaster, Tuya monitors all hosts, applications, services, networks and the like of the cloud platform through the O&M platform, and has a complete set of automatic process systems and guarantees for business failure; and a hot switch of multiple services guarantees that the service will not be interrupted.

A complete set of counter-measures has been developed for risks incurred by the software and hardware failure of the business system or even force majeure such as natural disasters, in order to guarantee the business sustainability under predictable conditions.

12.2 Disaster Recovery

Security, reliability and sustainable availability of business data are guaranteed by means of master-slave data real-time hot backup, redundant storage and multi-place backup. The backup is monitored and verified in real time manner.

Meanwhile, the rapid emergency switchover of business system and multi-chain standby system is guaranteed.

12.3 Emergency Plan

Tuya has developed internal emergency plans and measures for various assets and security risks, which Tuya implements in accordance with the Tuya Smart IT Emergency Response Procedure, in order to guarantee the correct, orderly and efficient afterward emergency handling, and guarantee the normal operation of works. The emergency plans include prior pre-plan procedure, monitoring and a series of fault secure measures. During the incident, providing sufficient data for subsequent handling by means of detailed

system monitoring review records is helpful to quick understanding and analysis, as well as corresponding interface personnel. After the incident, there is a complete set of handling procedures and emergency pre-plans to guarantee the rapid handling and analysis of problems as well as the responsibility investigation.

12.4 Emergency Drill

Tuya regularly carries out internal technical emergency tests and drills regarding large hardware failure, network DDoS, security incident and the like.

End of White Paper



©POWERED BY TUYA