



# Tuya Smart Information Security White Paper

Version 4.0.202010

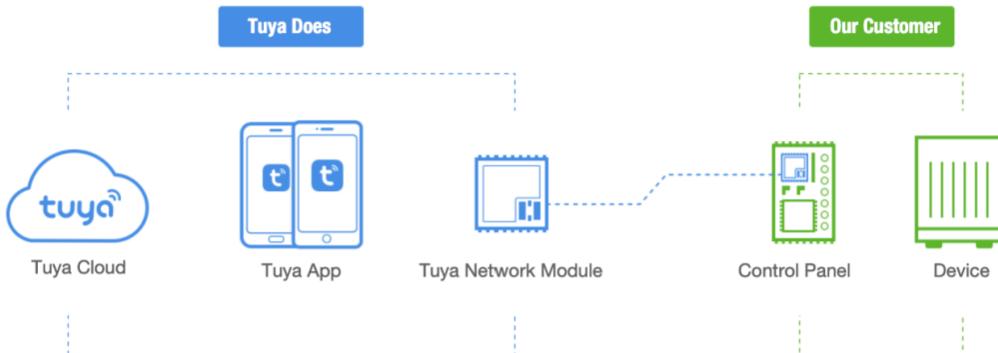
# Catalog

<b>1. INTRODUCTION TO TUYA SMART.....</b>	<b>1</b>
1.1 INTRODUCTION TO TUYA CLOUD PLATFORM.....	1
1.2 MISSION ON INFORMATION SECURITY ASSURANCE.....	2
<b>2. SECURITY RESPONSIBILITIES.....</b>	<b>2</b>
2.1 SECURITY RESPONSIBILITIES OF TUYA CLOUD.....	2
2.2 SECURITY RESPONSIBILITIES OF CUSTOMERS.....	3
<b>3. COMPLIANCE ENDEAVOR.....</b>	<b>3</b>
3.1 ISO 27001.....	4
3.2 ISO 27017.....	5
3.3 ISO 27018.....	5
3.4 ISO 9001.....	6
3.5 GDPR.....	6
3.6 CCPA.....	7
3.7 ENTERPRISE PRIVACY CERTIFICATE (EPC)- THE TRUSTE SEALED MEMBER.....	7
3.8 TEST ASSESSMENT OF "INTELLIGENT HARDWARE (IOT) OPEN PLATFORM".....	7
3.9 MORE COMPLIANCE EFFORTS.....	7
3.10 REGULAR COMPLIANCE ASSESSMENT AND AUDITING.....	8
<b>4. TUYA CLOUD PLATFORM OVERVIEW.....</b>	<b>9</b>
4.1 TUYA CLOUD INFRASTRUCTURE ARCHITECTURE.....	9
4.2 THE REQUIREMENT ON CLOUD SERVICE PROVIDER.....	10
<b>5. DATA SECURITY AND PRIVACY.....</b>	<b>10</b>
5.1 DATA SECURITY FRAMEWORK.....	10
5.2 DATA PROPERTY.....	11
5.3 DATA SECURITY LIFECYCLE.....	11
5.4 THIRD PARTY SECURITY AND PRIVACY ASSESSMENT.....	19
<b>6. SECURITY ORGANIZATION.....</b>	<b>20</b>
6.1 SECURITY AND PRIVACY TEAM.....	21
6.2 SECURITY AND COMPLIANCE COMMITTEE.....	21
6.3 HUMAN RESOURCE MANAGEMENT.....	21
6.4 SECURITY AWARENESS AND DISCIPLINE.....	22
6.5 TRAINING FOR SECURITY MANAGEMENT.....	22
6.6 IMPROVEMENT OF INFORMATION SECURITY CAPABILITY.....	23
<b>7. SECURITY ASSURANCE OF CLOUD PLATFORM.....</b>	<b>23</b>
7.1 PHYSICAL SECURITY.....	23
7.2 NETWORK SECURITY.....	24

7.3 INTRUSION PREVENTION.....	26
7.4 BUSINESS SECURITY AND RISK CONTROL.....	29
<b>8. SECURITY DEVELOPMENT LIFECYCLE MANAGEMENT (SDLC).....</b>	<b>31</b>
8.1 SECURITY DEMAND ANALYSIS AND PRODUCT DESIGN.....	32
8.2 DEVELOPMENT STAGE.....	32
8.3 SECURITY TEST, FIXING AND VERIFICATION.....	35
<b>9. SECURITY OPERATION AND MAINTENANCE.....</b>	<b>36</b>
9.1 SECURITY RISK MANAGEMENT.....	37
9.2 ACCESS CONTROL.....	40
9.3 SECURITY MANAGEMENT OF SERVICE PROVIDER.....	42
9.4 CUSTOMER SECURITY SERVICE SUPPORT.....	42
<b>10. TERMINAL SECURITY.....</b>	<b>42</b>
10.1 APP.....	42
10.2 HARDWARE AND FIRMWARE SECURITY.....	44
<b>11. BUSINESS SUSTAINABILITY.....</b>	<b>46</b>
11.1 BUSINESS SUSTAINABILITY.....	46
11.2 DISASTER RECOVERY.....	46
11.3 EMERGENCY PLAN.....	46
11.4 EMERGENCY DRILL.....	47

## 1. Introduction to Tuya Smart

Tuya provides a leading global AI+IoT platform that brings smart products to life for manufacturers, brands, OEMs and retail chains. The platform offers hardware access, cloud services and app development. Tuya also helps brands upgrade their technology and business models, enabling them to deliver smart devices to meet consumer demand.



By the end of October 2019, Tuya serves more than 180,000 developers in over 190 countries powering over 90 thousand product SKUs such as lighting, appliances, and surveillance equipment. Powered by Tuya products covering 500 types of products, ranking No.1 in the world. European and North American markets account for almost 50% of the business. Tuya is internationally operated, with local headquarters in the U.S., India, Germany, Japan, Colombia and China. The Tuya Cloud processes over 40 million daily AI voice interactions from its five global data centers. The average per-command processing time is 0.01 second from the Tuya cloud, 10-30 times faster than the industry average.

### 1.1 Introduction to Tuya Cloud Platform

Tuya Smart deploys cloud services around the world and is committed to providing safe, stable, and fast cloud services for customers worldwide. It is capable of concurrently processing hundreds of millions of massive data and delivering uninterrupted computing services of up to 99.99% availability. Tuya integrates global nodes from different cloud platforms to allow users in different regions to access the nearest nodes, which ensures efficient and stable user experience.

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

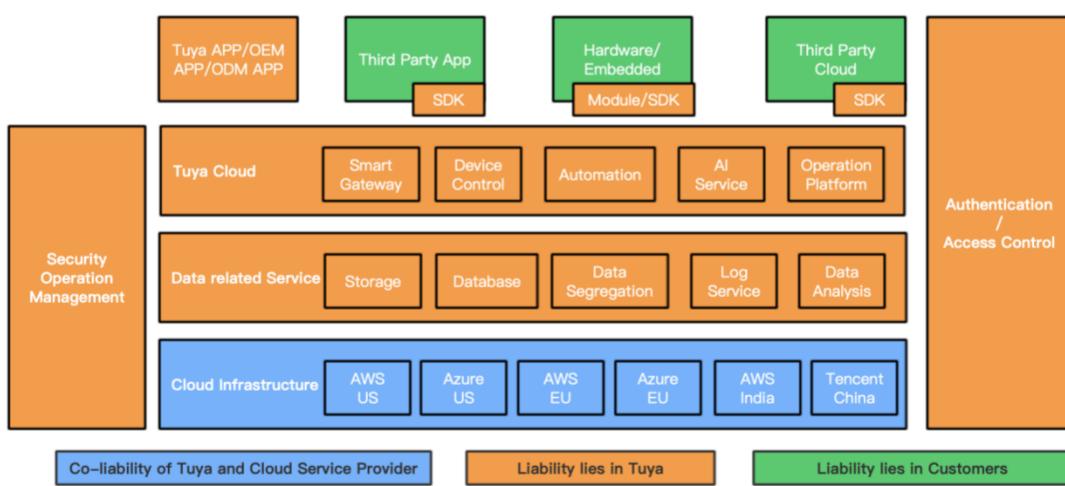
Tuya is devoted to providing customers with consistent, reliable, secure and conforming IoT access services, and guaranteeing the availability, confidentiality and integrity of the data of users. Tuya Cloud's promise: Tuya Cloud has data protection at its core and is built on cloud security. It relies 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 aims to provide customers with in-depth understanding of Tuya and in-depth security insight of Tuya Cloud.

## 2. Security Responsibilities

Tuya is liable for security operation for services and data exchange on Tuya Cloud and takes responsibility for security of the cloud service platform and infrastructure. When it comes to embed software for Apps or hardware developed by customers (including by use of SDK) access to Tuya Cloud, the customers will have to guarantee the application and data (see section 2.2), including the security and compliance of hardware and App. The diagram below shows how the liability is shared among infrastructure cloud service providers, Tuya, and customers.



### 2.1 Security Responsibilities of Tuya Cloud

Tuya Cloud ensures the security of the whole infrastructure, operation and physical implementations by using industry-leading cloud hosting provider Amazon, cloud computing platforms MS Azure, as well as Tencent Cloud, a China's leading technology

company.

Tuya Cloud covers data security and cloud service security, and Tuya security team promises to play to the fullest on the security matter and, bring 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. This omission 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 Digitization Standardization Technical Committee (SAC/TC 426) in China.
- 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 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 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.

### 3.2 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.

### 3.3 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).

### 3.4 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.

### 3.5 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 took 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 Enterprise Privacy Certificate (EPC)- the TRUSTe Sealed Member

Becoming TRUSTe certified means Tuya is adequately implementing policies around data privacy and governance. With this certification, Tuya has stepped up to the next level of data and privacy adherence and has proven yet again to be an IoT platform that is secure and trustworthy.



### 3.8 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.



### 3.9 More Compliance Efforts

Tuya has a dedicated security and compliance team that closely tracks industry trends, and immediately respond to major global security and compliance standards, as well as data security and privacy regulations in various countries. Constantly, Tuya would cooperate with third-parties, technology consulting companies or service groups, as well

law firms focusing on data protection help test and assess, as well as give a guidance to Tuya on how to fully conform with the requirements. In recent years, including data protection regulations in Russia, India, etc., as well as IoT-specific regulations in the United Kingdom, California U.S., and Washington U.S., Tuya has conducted strict internal self-assessment and evaluation to ensure that all Tuya's services and products can meet these requirements.

### 3.10 Regular Compliance Assessment and Auditing

In order to ensure the continuous and effective operation of the company's information security management system and privacy & compliance framework, Tuya has dedicated compliance supervising personnel who conduct internal audits at least once a year, and inspection, supervision and evaluation of the internal control, compliance assessment and risk management at the organizational level, to verify whether the company's information security management activities meet the requirements of ISO/IEC27001:2013, ISO/IEC27017:2015, ISO/IEC27018:2019, AICPA SOC2 and other standards, and whether they meet the requirements of GDPR, CCPA and other relevant laws and regulations. In further to ensure its effectiveness of the information security management system, and implement rectification and improvement based on the findings.

## 4. Tuya Cloud Platform Overview

### 4.1 Tuya Cloud Infrastructure Architecture



The fundamental infrastructure of Tuya Cloud is provided by Amazon and Microsoft, and is integrated with global service nodes. In terms of features on the platform, starting from hardware integration phase, Tuya Cloud provides the service capability with a whole life-cycle coverage, including product definition, simulation test, hardware development,

client development, cloud platform interaction, product testing, operation management, and data analysis. In terms of cloud 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.

## 4.2 The Requirement on Cloud Service Provider

In terms of choosing Tuya cloud service provider, we will take the following criteria into consideration:

1. The world-renowned cloud service provider brand, leading the world in technology.
2. Secure and stable cloud computing products .
3. Equipped and constantly comply with the complete information security standards, and global legal and qualification certificates.

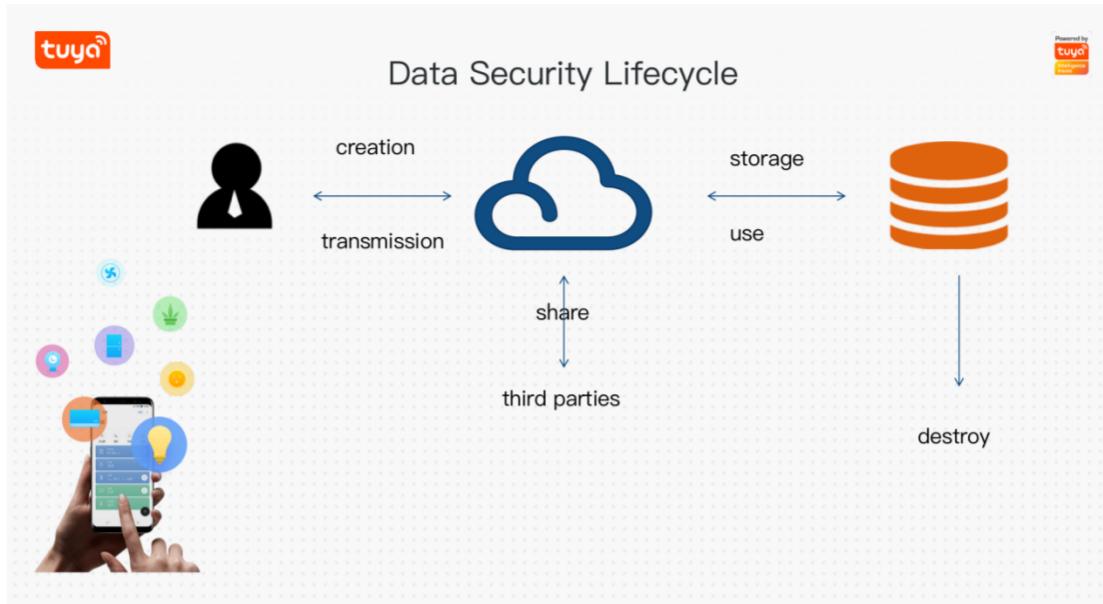
The cloud server providers currently under contract are Amazon, Azure, and Tencent Cloud.

## 5. Data Security and Privacy

### 5.1 Data Security Framework

Tuya beholds the philosophy that "centralizing customer value", and pays particular attention to establishing long-term and lasting trust relationships with customers. From the perspective of data security life cycle, the cloud data security system adopts both organizational management and technical means to carry out comprehensive and systematic construction. Data security management are carried out at all phases of the data life-cycle (data collection, storage, processing, transmission, sharing, and deletion) to achieve data security goals.

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



## 5.2 Data Property

Tuya is committed to the protection of data privacy, in compliance with all data protection laws, the individual user is the owner of the ownership and ownership of data belonging to individual users. Respectively, in the customized solution, the personal data generated shall be controlled by the respective customers, namely the data controllers. The customer has the discretion to determine the way and purpose of processing personal data, in the meanwhile, the customer has the primary liability in ensuring data security and conformity of privacy. Tuya acts as the data processor and The data processing activities are implemented under customers' written instruction, which is elaborately documented in the data processing contracts or addendum, on the lawful and transparent basis. Therefore, given compliance with the data protection regulations and Tuya privacy policy, Tuya is surely able to assist clients and users in protect data confidentiality, integrity, and security.

## 5.3 Data Security Lifecycle

### 5.3.1 The fundamental principles of processing personal data,

Generally speaking, the data processing principles are set out in majority of data protection laws and regulations, including:

Lawfulness, fairness and transparency; Purpose limitation; Data minimization; Accuracy; Storage limitation; Integrity and confidentiality; Accountability principle.

The principles can be illustrated by the following information.

### 5.3.2 Individual Privacy Rights

Data security and privacy protection laws and regulations emphasize the protection of personal privacy rights. Tuya has formed the "Procedures of Handling Personal Privacy Rights" to help realize users' privacy rights based on the provision of services. At the same time, Tuya also provides assistance to customers in responding to user requests, including the following privacy rights:

#### 1) Right to be Informed

- ◆ The Privacy Policy can be found here for more:  
<https://auth.tuya.com/privacy?from=http%3A%2F%2Fiot.tuya.com%2F>. the mandatory element to be included in a compliant privacy policy shall describe the
  - ✓ The privacy Policy elaborates the type of personal data being collected and what service relies on these type of data, as well as the purposes of processing personal data.
  - ✓ The prompt shall be displayed or a communication email shall be delivered to the users when a user registered in the App and, when the significant change has been made on the way or purposes of processing personal data, or on the new type of data collection, a separate consent shall be made by the user.
- ◆ Cookies Statement on the website

The Cookie Statement on Tuya IoT website performs a valid user consent mechanism following e-Privacy Regulation.

#### 2) Right of Access

Users can access personal data collected by Tuya through the App without additional technical support.

Users can make a privacy request to Tuya for any data processing activities and its related purposes, as well as all personal data associated with services and functions.

#### 3) Right to Erasure

As the owner of the data, the user can delete the data completely through the account deletion function on the APP or through submitting feedback/contact the official website customer service. The deleted data includes but is not limited to user identity information, the user's use of APP and smart device records, and the information generated and collected by the smart device during the user's use.

#### 4) Right to Rectification

Users can manually and proactively rectify the personal data on the App if there is any incorrect or out-of-date information about the individual.

## 5) Right to Data Portability

If a user wish to export all personal data and transfer to another data recipient for data processing, Tuya can assist data extraction for the user.

### 5.3.3 the Security Management through Data Lifecycle

#### 1) Data Collection

Tuya adheres to the principles of data protection and personal privacy rights. The user's consent for data collection constitutes the legal basis for data further processing. Data collection is performed by protecting the user's Right to be Informed and the necessary principles of the service.

#### 2) Data Storage

##### ■ Data and File Storage

Tuya Cloud will logically isolate data to ensure the security of customer data. At the same time, Tuya Cloud provides different data storage services under various business scenarios. Personal data is encrypted and stored using AES256. Personal identity data will be desensitized and data categorized as highly sensitive will be secured with irreversible algorithm. At the same time, the key is uniformly secured through the key management system (KMS) and further managed and distributed through the KMS.

For sensitive data, such as images or videos, Tuya will protect with generation of unique keys based on specific users and specific devices to encrypt the data.

##### ■ Data Storage Location

Tuya implemented 6 data centers, China Server Room, AWS West USA, Azure East USA, and AWS in Europe and India Server Room (with data centers physically isolated from each other), providing data services according to user's location. More server rooms will be made available in the future.

- China: The data is stored in Tencent Cloud Shanghai, China, and basic cloud computing support is provided by Tencent.
- USA: Tuya has deployed two data centers in USA, the west one in Oregon AWS, and the east one in MS Azure Virginia. By default, the data will be hosted in AWS while if the customer .
- Europe: Tuya has deployed two data centers in EU, the AWS Frankfurt, Germany, and Azure in Netherlands.

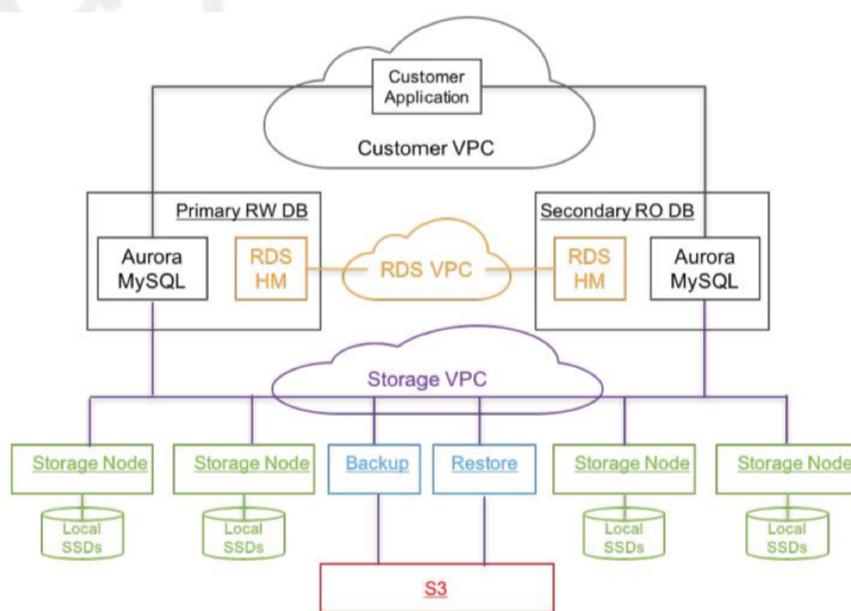
- India: The data is stored in a server center in Mumbai, India, and basic cloud computing support is provided by Amazon AWS.

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

#### ■ 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. It allows high reliability and availability of data and services from the physical perspective.

Tuya uses cloud databases for data storage, the default master-subordinate reproduction, the master and subordinate databases are distributed in different availability zones. All disks use local SSD hard disks and support automatic disk expansion. The full and incremental backups of data are all stored on cloud.



For data backup and synchronization across computer rooms, strict data integrity checks will be performed to ensure the integrity of synchronized or backup data.

### 3) Secured Data Processing

#### ■ Data Classification

Referring to “Tuya Information Classification and Handling Process” and specific categories of personal data, application data as well as corporate business data are

defined accordingly, different security means has been taken to different categories of data.

#### ■ Access Control Mechanism

- Tuya Cloud adopts access control mechanism relying on the Access Control Platform. Including the unified control of the application, and assigning the minimum and least necessary permissions according to the user roles and responsibility.
- Implement internal approval process for sensitive data operations.
- Separate the roles of security managers, data operators, and auditors.

#### ■ Data Filtering

Tuya Cloud enforces strict verification of the type, length, format, etc. of the data of all entrances to ensure the integrity of the data and not be tampered.

#### ■ Data Auditing

Complete data usage records, including auditing records of applications or user operations. For high-risk data processing, the corresponding supervisor and compliance auditor needs to approve before it can be executed.

#### ■ Data Dashboard

In principle, the raw data is not allowed to be displayed in the IoT platform or other dashboard. Therefore, measures such as de-identification or desensitization have been adopted. Specific business scenarios require displaying personal data, or respond to customers' data specific display needs, Tuya prevents it by mouse sliding or clicking display so as to reduce the risk of personal information leakage during the operation.

#### ■ Data Desensitization

After collecting personal data, Tuya will perform de-identification processing, and adopt technical and management measures to store the de-identified data separately from the data that can be used to restore the identification of the individual, and ensure that the subsequent processing of personal data does not re-identify the individual.

### 4) Data Retention Policy

The retention period of personal information is the minimum time necessary to achieve

the purpose for providing product and service. Tuya will delete or anonymize user data at the request of the customer, and return the data to the customer when the data retention policy triggers. Therefore Tuya has adopted the principle of minimum data retention:

- The retention of user's personal data is limited to the user's express consent so that the personal data can be used for service-related purposes, and shall not be used for any additional purposes without the user's consent.
- Data that needs to be retained in accordance with the law, or the company has the ability to prove that it is necessary for business purposes, can be retained within the time specified by a clear data retention schedule.
- Data retained for realizing the legitimate interests of customers or third parties can only be retained when the company has clear contractual agreements or instructions with customers or third parties, such as when providing services to customers or providing services for other purposes.
- According to the principle of minimum data retention, customers have the right to determine data retention strategies and inform Tuya in time for service purposes. When customers request to delete data or return data, Tuya will follow this clear instruction to execute.

#### 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 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.

- Once the memory and disk that have stored customer data are released and recovered, all their information will be automatically overwritten with zero values. At the same time, any replacement or obsolete storage devices will be degaussed and physically destroyed by the cloud server infrastructure provider.

#### 5.3.4 the Technical Measures for Data Security and Privacy

- 1) Data Secured Transmission
  - The integrity of the data transmission

When the application program processes the data transmission process, it will perform integrity check, usually using the HMAC-SHA256 algorithm.

■ The desensitization and encryption of the data content

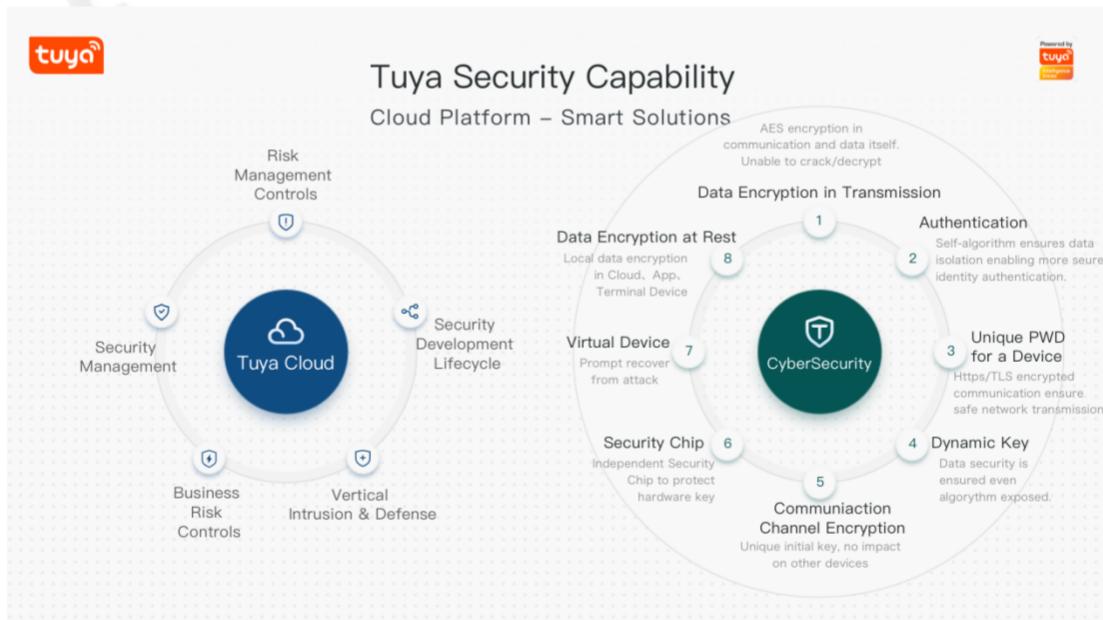
AES-128 encryption is utilized in the communication between the APP and the cloud, the communication between the device and the cloud, the communication between the APP and the device, as well as the communication between the device and the device, the sensitive data, including passwords, biometric data, etc., are transmitted after being desensitized by an irreversible algorithm.

■ Encryption of the Transmission Channel

Tuya uses the TLS1.2 protocol for communication channel, the communication between the APP and the cloud, the communication between the device and the cloud, whether it is HTTP or MQTT, and implements strict certificate verification.

## 2) Data Security on the Device End

Tuya Cloud provides multiple security strategies to ensure the security of data generated by smart devices. As shown below:



■ In terms of protection on the device-cloud interaction:

- Data encryption: AES -128 is adopted for data content encryption.
- Identity 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, including dynamic key and dynamic password, to ensure device security.
  - Transmission encryption: TLS1.2 data encryption transmission protocol and mutual mandatory authentication.
  - Secure chips: part of modules support using the secure chip versions to have secure storage for authorized information and encrypted key, etc.
  - Virtual device design: it guarantees the devices will not be affected even the authorized information about the device is corrupt, meanwhile, Tuya adopts pseudonymization technology in device id to ensure user privacy and security.
- In terms of interaction between devices in LAN:
- Data encryption: AES-128 is adopted for data content encryption before data transmission in LAN.
  - Dynamic key: Dynamic distribution of algorithm during network configuration.

The details about the Security of Cloud Platform can be found in Chapter 7.

The details about the Security of Device can be found in Chapter 10.

### 5.3.5 The Organizational Measure for Data Security and Privacy

#### 1) The International Data Transfer

With the ever-changing requirements for data security and privacy protection in the international environment, Tuya pays close attention to the international dynamics of cross-border data transmission in real time. For example, the standard data cross-border agreement issued by the European Union guarantees the legal basis for data transmission from the EU region to other regions. Tuya also pays attention to the legal compliance basis for data transmission in other regions/countries/regions and responds in a timely manner.

In general, Tuya strictly follows the general principles of "data localization requirements", and user personal data is stored on the local server to the greatest extent and would not be synchronized to other regions.

In view of Tuya's business management and business needs, Tuya has the authority to process data in various data centers. This type of data processing also constitutes cross-border data transmission. However, for this type of remote access to data, data

protection laws and regulations are fully recognized and comply with data cross-border transmission regulations;

## 2) The Access Control for Data Processing Activities

In accordance with the principle of "minimizing data processing access", Tuya strictly manages the personnel who have access to customers' personal data, clarifies the division of responsibilities, standardizes data processing procedures, regularly reviews access, and strengthens data security training.

### 5.3.6 Data Sharing

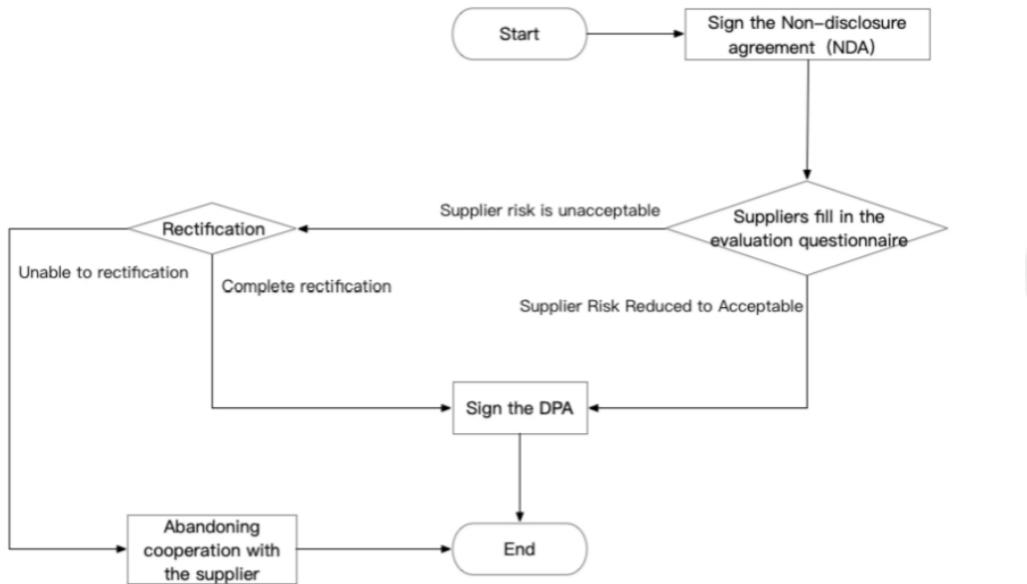
Tuya conducts data sharing with third-party service providers or partners based on the needs of various service scenarios and under the premise of lawfulness and reasonableness, mainly including:

- Third-party smart features, such as Google and AWS, require users to actively authorize their account data to be shared to the corresponding voice platform, so as to realize support for smart home scenes of Tuya platform users like Google Home, AWS Echo, etc.
- Third-party software service providers, such as SMS and phone service provider Nexmo, mobile push services from Google or Apple, Tuya tries to minimize the data shared with the service providers, only required for this part of the service. If it involves the sharing of personal data, Tuya conducts strict security and compliance assessment over the service provider, including audits of privacy and data security.

In principle, sharing of user personal information is prohibited. If sharing is required for special reasons based on the contracted service provided for the user or legitimate basis, a comprehensive privacy impact assessment should be conducted on the third party. At the same time, the user needs to be informed of the purpose of sharing personal information, the type of data recipient, and the personal information subject's authorization and consent should be obtained in advance.

## 5.4 Third Party Security and Privacy Assessment

In the complete services provided by Tuya, Tuya authorizes a trusted third-party to perform necessary data processing activities. An assessment of data security and privacy protection in accordance with the "Internal Third Party Risk Assessment Process" is implemented. The review generally includes GDPR evaluation and PIA/DPIA evaluation based on product or project. The evaluation process is roughly shown as follows:



With the help of TrusArc's privacy compliance assessment tool, we first adopt the standard version of the security and privacy compliance questionnaire (below) to conduct a standardized assessment of third party. When a third party has an non-compliance item which impact the service, it without any doubt shall be resolved before the service commences, otherwise they will not be allowed to enter the third party's list.

Status	No.	Question	Comments	Attachments	Labels	Create Tasks	Not Set
<span style="color: green;">●</span>	1	Describe the key products and/or services delivered by your organization.	0	0	0	<span style="border: 1px solid #ccc; padding: 2px;">Create Tasks</span>	<span style="border: 1px solid #ccc; padding: 2px;">Not Set</span>
<span style="color: green;">●</span>	2	Select the key industries that your organization operates within.	0	0	0	<span style="border: 1px solid #ccc; padding: 2px;">Create Tasks</span>	<span style="border: 1px solid #ccc; padding: 2px;">Not Set</span>
<span style="color: green;">●</span>	3	Please describe the industry your organization operates within.	0	0	0	<span style="border: 1px solid #ccc; padding: 2px;">Create Tasks</span>	<span style="border: 1px solid #ccc; padding: 2px;">Not Set</span>
<span style="color: green;">●</span>	4	How long has your organization been in business?	0	0	0	<span style="border: 1px solid #ccc; padding: 2px;">Create Tasks</span>	<span style="border: 1px solid #ccc; padding: 2px;">Not Set</span>
<span style="color: green;">●</span>	5	Indicate the specific countries where your organization maintains a physical presence.	0	0	1	<span style="border: 1px solid #ccc; padding: 2px;">Create Tasks</span>	<span style="border: 1px solid #ccc; padding: 2px;">Not Set</span>

## 6. Security Organization

To enhance the security awareness of all the employees and to guarantee customer interests as well as product and service reputation, Tuya advocates "Everyone has the liability to protect information security" as the common concept and, a best practice to cultivate the culture. This culture is embodied throughout every human resources activity,

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 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 Corporation before, a US financial service company. Meanwhile, Tuya invited external professional privacy and security consultancies on 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 Security and Compliance Committee

Tuya has established an Security and Compliance Committee as an oversight role, which is led by key founders, including the CEO, CTO, CFO and other senior management to jointly overseeing information security and privacy compliance, and to formulate unified goals ahead. Compliance with regulations and compliance requirements are the baseline, providing risk and compliance support for Tuya (including operational and business stakeholders).

Tuya Security and Compliance Committee conducts a formal meeting at every quarter to assess the security and compliance work and as well as alignment of the goals, and provide support for the development of compliance work.

### 6.3 Human Resource Management

Tuya human resource management framework is consistent with global human resource management framework of the company. At the same time, the ruling Basic Policy of Human Resources regulates the whole human resource management processes, in recruitment, management of employee contracts, attendance and performance management, and procedural management of resignation to strengthen human resource security.

The role of human resource department in ensuring security mainly includes ensuring that employee background and qualifications meet business requirements. All employees act are lining with code of conduct, with the requirements of all the laws, policies, processes and set out by Tuya. All employees have necessary knowledge, skills and experience to fulfill their duties.

The employment agreement that between the employee and Tuya complies with the terms of the information security policies. At the same time, a confidentiality agreement must be supported to ensure the confidentiality and integrity of information, whether it's about Tuya's or customers, that the employee may have access to, including commercial secrets, technical secrets, employee information and customer data.

#### 6.4 Security Awareness and Discipline

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.

Tuya "Employee Information Security Handbook" supports employees' security awareness and code of conduct, a quarter assessments and education will be conduct which aims to regulate employees' disciplines over handling information security matter. Public commendation or warning will be given to employees who exceeding the expectation on information security protection or who violate security policies and procedures.

#### 6.5 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. Each employee has to pass the online training quiz, employee shall continue learning until they pass the quiz.

Information security awareness training is presented online and offline, including but not limited to security development training, penetration testing training, vulnerability training, security architecture training, privacy and compliance training, security development process training, etc.

## 6.6 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 as a data center, ensuring 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 6 available regions with coverage of China, Europe, the east US, the west US and India according to domestic and overseas marketing needs and in combination with submarine optical cable distribution and measurement in cities in the world.

It includes but are not limited to the AWS Oregon server room in west US and Azure Virginia in east US server room; AWS Frankfurt and Azure Amsterdam server room in

Europe; AWS Mumbai in India and Tencent Shanghai, China; and other server rooms in Hong Kong, Singapore, Tokyo, and São Paulo may further expand in future (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

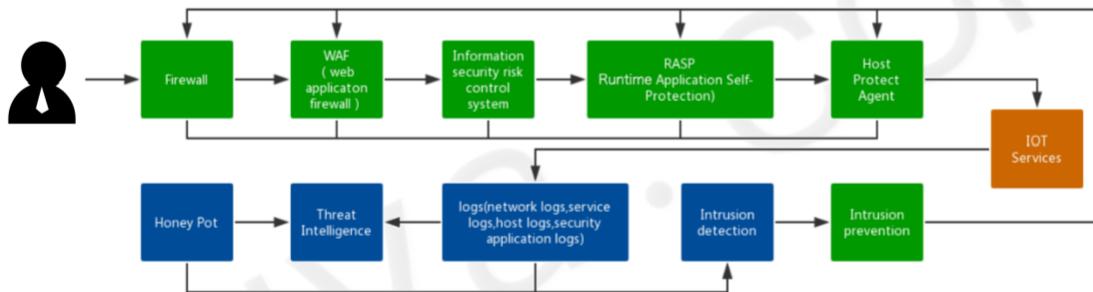
Security event management: physical security emergency plan is developed with the platforms of the cloud server providers, and the operators at data center are organized regularly for security drill. In case of a physical security event, the plan will be carried out immediately to guide relevant personnel 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 including the communication between Device and Cloud, the API interface is also equipped with a full range of TLS. In the meantime, the AES 128 is applied to its content, the key is randomly generated based on each device and a user, ensuring the uniqueness and security of the key, two-layer encryption ensures the communication channel.

### 7.2.3 Network Isolation and Access Control

Tuya has established an 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.

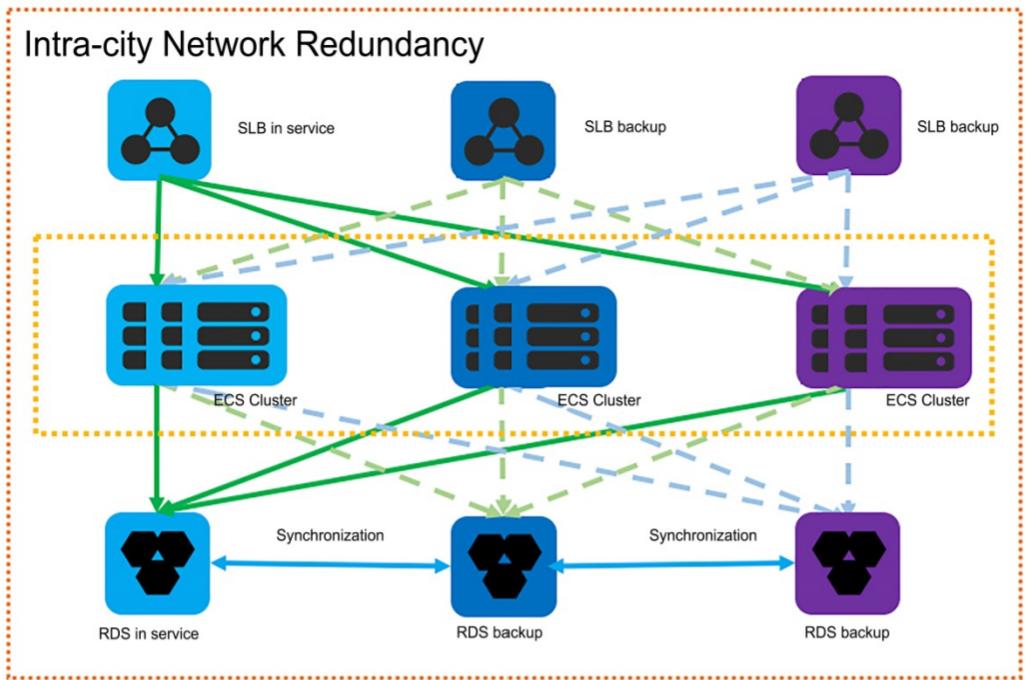
With regards to the network access isolation for cloud users, Tuya provides multiple security mechanisms including virtual-control-level resource access control policy, inter-private network isolation policy in cloud platform, Web console permission distribution and authentication, interface conversation 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 (Challenge Collapsar), check all abnormal IP address by analyzing all request logs and threat intelligence data of third parties and dynamically shield suspicious source address.

## 7.3 Intrusion Prevention

### 7.3.1 Internet Intrusion detection

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.

server name	Interception time	Real IP	Access host	method	response	Request uri	UserAgent
Http://xxx.xxx.xxx.123	2019-08-07 16:30:48	192.168.1.100	www.tuya.com	POST	200	/api/v1/devices	Mozilla/5.0 (Windows NT 6.1; Trident rv:11.0) like Gecko
Http://xxx.xxx.xxx.123	2019-08-07 16:07:00	192.168.1.100	www.tuya.com	GET	200	/api/v1/devices	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 9.0; Windows)
Http://xxx.xxx.xxx.123	2019-08-07 15:36:18	192.168.1.100	www.tuya.com	GET	200	/api/v1/devices	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 9.0; Windows)
Http://xxx.xxx.xxx.123	2019-08-07 15:36:14	48.88.55.111	www.tuya.com	GET	200	/api/v1/devices	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 9.0; Windows)

### 7.3.2 Internet Intrusion Prevention:

Intrusion blocking is performed through security protection tools such as network firewall, WEB application firewall (WAF), MQTT application firewall (EWAF) and RASP.

WAF and EWAF can analyze the data flow of application requests, match and intercept through rules.

#### WAF Rule Management

Mode selection	Sync configuration	Apollo configuration	Redis configuration	Rule switch
Slave node	Synchronization time (seconds) 60	State Enable  Schema http  Domain www.tuya.com  Port 8080	IP 192.168.1.100  Port 8080	<input checked="" type="checkbox"/> WAF switch <input checked="" type="checkbox"/> Source IP acquisition <input checked="" type="checkbox"/> IP black and white list <input checked="" type="checkbox"/> Referrer interception <input checked="" type="checkbox"/> URI filtering <input checked="" type="checkbox"/> Header filtering <input checked="" type="checkbox"/> UA filtering <input checked="" type="checkbox"/> Cookie filtering <input checked="" type="checkbox"/> QueryString filtering <input checked="" type="checkbox"/> QueryString pollution filtering <input checked="" type="checkbox"/> Form filtering <input checked="" type="checkbox"/> Form pollution filter <input checked="" type="checkbox"/> CC attack protection

RASP (application runtime self-protection) can be directly applied to the service of the protected application to provide function-level real-time protection, which can detect and protect unknown vulnerabilities without updating the mechanism and upgrading the

protected application code.

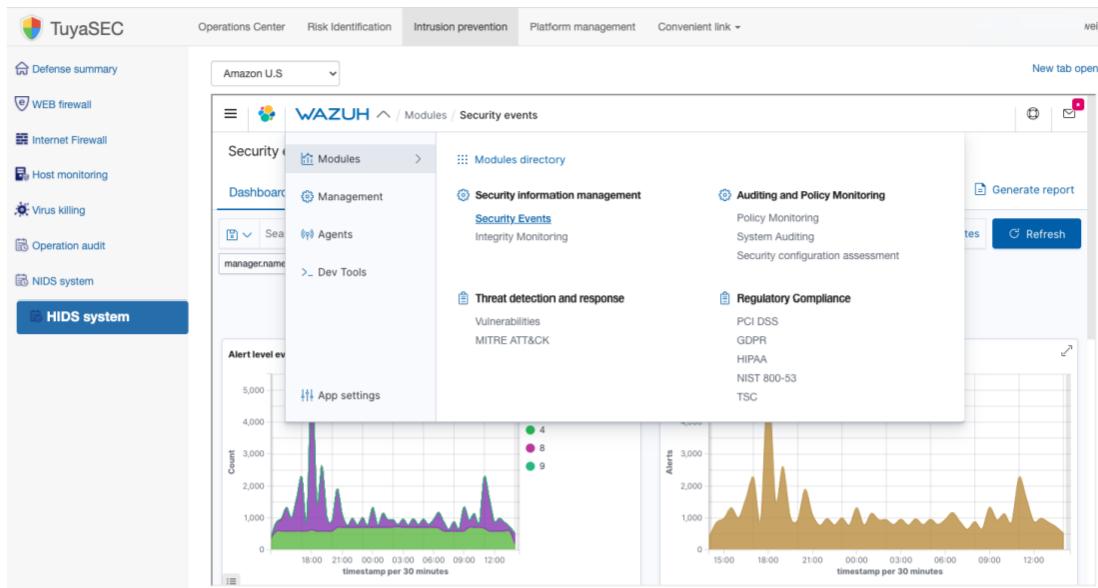
15022 results, displayed page 1 of 1502

ATTACK TIME	URL	SOURCE OF ATTACK	ATTACK TYPE	ALARM MESSAGE	OPERATING
2020-09-03 14:34:22	/a-hart/dat	3	SQL injection	SQLi - SQL query structure altered by user input, request parameter name: input_json->sqlConfig->drillFields->2->title, value: 一级品类code	<a href="#">see details</a>
2020-09-03 14:34:22	/a-hart/dat	239	SQL injection	SQLi - SQL query structure altered by user input, request parameter name: input_json->sqlConfig->layers->0->y->1->realAliasName, value: 二级品类code (计数)	<a href="#">see details</a>
2020-09-03 14:34:22	/a-hart/dat	.73	SQL injection	SQLi - SQL query structure altered by user input, request parameter name: input_json->sqlConfig->layers->0->y->0->realAliasName, value: type (求和)	<a href="#">see details</a>

### 7.3.3 Host Security Detection

Host computer supervision: including WEB SHELL 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.

IP address	Login area	Login IP	Login user	Log in time	Login hostname
...	...	...	rjgn	2020-09-12 14:25:55	jc-bastion
...	...	...	...	2020-09-12 1f	jc-bastion
...	Shen...	...	wan...	2020-09-12 10:12:47	jc-bastion
47...	...	...	w...	2020-09-12 10:11	pc-bastion
...	...	...	...	2020-09-12 10:12:47	jc-bastion
...	...	...	...	2020-09-04 14:56:26	...
...	...	...	...	2020-09-04 14:43:38	...
47...	...	...	...	2020-09-04 14:39:09	...
...	...	...	...	2020-09-03 15:49:56	...
47.92.1.101	Shanghai	112.95.129.11	...	2020-09-21 14:48:26	...



### 7.3.4 Database Audit

The internal database management system has formulated a 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.

### 7.3.5 Virus Inspection

Regular check the file storage server for file security, virus inspection, or executable files.

## 7.4 Business Security and Risk Control

### 7.4.1 Account Security

Account security is the foundation of the Tuya Cloud service system, therefore, the security control and log audits have been implemented 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 strategy protection is carried out against common account risk sources such as database collision and API abuse.

At present, all login-related interfaces such as login and reset password use invisible or sliding verification codes to ensure the ability of business man-machine identification and prevent malicious registration, database collision and other attacks.

At the same time, the weak password is checked during user registration, and the setting of common weak passwords is prohibited.

#### 7.4.2 Device Authentication

When Tuya module is produced, it will write a pair of device authentication information, which is unique in all devices, and is bound to the environment of the module, including chip ID and MAC address, etc., in each session request, information was added when signing the data package. Each communication must ensure the accuracy of the module's environmental information and equipment certification information to be able to communicate effectively.

#### 7.4.3 Content Security

Tuya has carried out a unified business file type identification, virus scanning, and Trojan scanning engine at all file upload entrances, which can quickly identify the security risks of uploaded files.

#### 7.4.4 Key Management

Tuya has a safe and reliable key management system and complete key lifecycle management, including creation, activation, deactivation, conversion, distribution, backup, destruction, etc. At the same time, data is encrypted and stored based on key.

On the smart device side, the initial key information is written into the security area of the device, and after the device completes authentication and user binding, a random key is generated. Meanwhile, the key used to encrypt data locally on the device is randomly generated from the device information and is only valid locally.

There is a unified key management system KMS in the cloud to support the creation and management of keys, which can effectively protect the confidentiality, integrity and availability of keys. At the same time, it has a complete audit function to meet regulatory and compliance requirements.

#### 7.4.5 Certificate Management

For server and terminal equipment certificates, Tuya has developed a set of certificate management system. The client for supporting certificate can implement code deployment through the client to achieve the trusted call and configuration. In the meantime, the certificate management system encrypts and stores certificates and other information, providing business support based on domain name, terminal information, firmware information and other certificate issuance, verification and other functions.

#### 7.4.6 Configuration Management

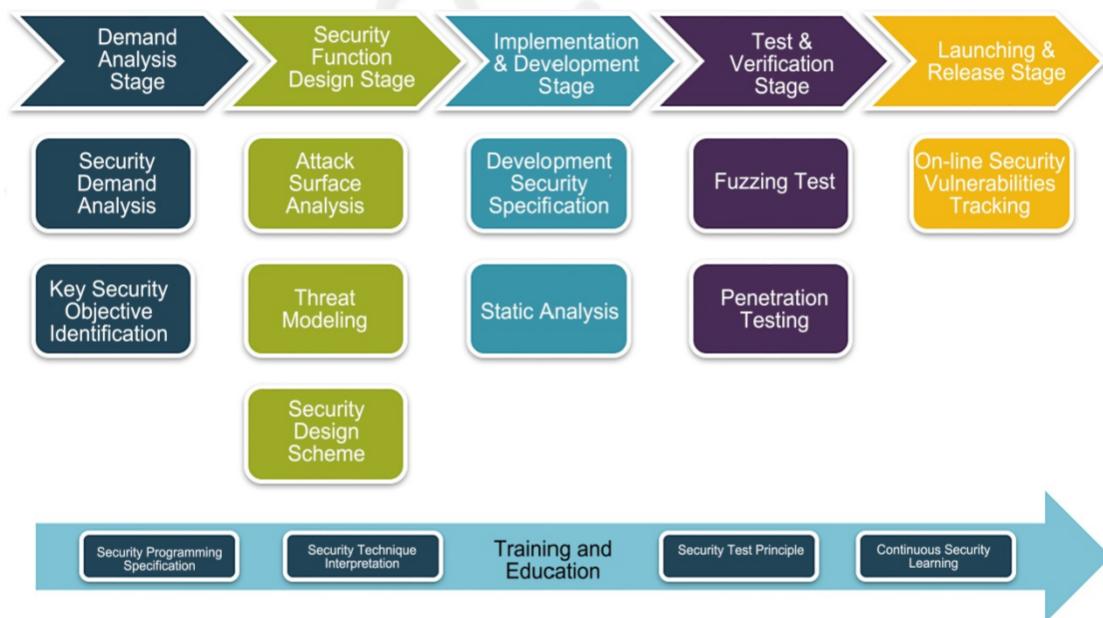
Tuya does not allow any hard-coded configuration, including secret keys, certificates, database configuration and other information. All configurations need to pass application

authentication and then access the configuration center to pull the corresponding configuration. The configuration center is connected to the certificate management and key management system to realize unified configuration management. At the same time, for each application's authentication and access management, a specific approval process is required before business calls are allowed.

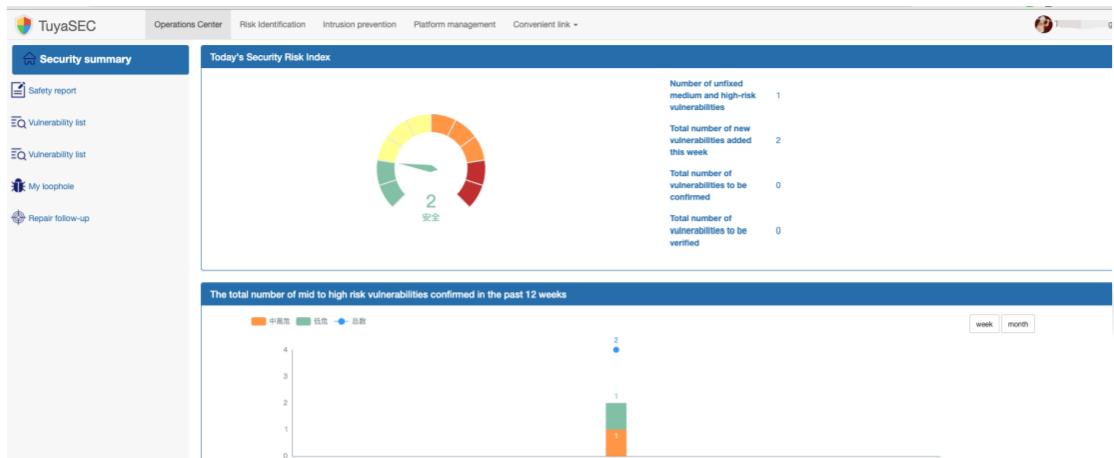
## 8. Security Development Lifecycle Management (SDLC)

Tuya develops three-terminal services and products of cloud, APP and smart devices in accordance with the security development lifecycle management, with the goal of integrating information security into the entire SDLC.

Tuya SDLC fully covers all stages of the system development lifecycle.



Unified project SDLC 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, 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 security team will analyze the system attack surface, establish a threat model and security&privacy risk assessment, 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.

Tuya security coding standard follows the international coding standards, including the relevant standards of the USA National Standards and Technology Association NIST, the relevant standards of the European Telecommunications Standards Institute ETSI, and the relevant standards of OWASP.

### 8.2.2 Code Auditing

The code auditing 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.

The screenshot shows the TuyaSEC Operations Center interface. On the left, there's a sidebar with various scanning options like Asset details, Black box scanning, Code audit (which is selected), Mobile scan, Mirror scan, POC scan, Space scan, Leakage of sensitive information, and Security tools collection. The main area has tabs for Asset safety summary, Risk identification, Intrusion prevention, Platform management, and Convenient link. A search bar at the top right allows searching by project name/version. Below the search bar is a table with columns: Asset name, Asset ID, version, Audit record, Vulnerability list, status, and operating. The table lists 1737 records. At the bottom right, there are buttons for New scan and Rule management, and a page navigation section showing pages 1 through 174.

At the same time, Tuya also integrates the international mainstream third-party code audit tool, which supports Tuya's main language through this tool, which can effectively help the business to find vulnerabilities.

The screenshot shows the Qianxin Codewise platform. At the top, there are tabs for Home, Quick check, Report management, Statistical Analysis, System Management, Current user, and Download. The Home tab is active. Key statistics are displayed: 2449 total tasks initiated, 12,295.69 million lines of detection code lines, and 272 cumulative running days. Below this is a section for Test language statistics, showing a pie chart and a table of languages and their line counts: Java (110,828,700 lines), C/C++ (8,595,200 lines), Python (147,400 lines), Objective-C (305.96 million rows), and NodeJS (326,000 rows). The next section is Defect detection, showing 1.4 million defects detected, 13.36 million high-risk defects, and 22.15 Wan. It includes a donut chart and a list of top 10 defects: Path traversal, Cross-border access, Improper loop termination, SQL injection: MyBatis, Unsigned integer wrap, Stored XSS, Null pointer dereference, and XSS for communication net.

### 8.2.3 Open Source Auditing

Tuya's self-developed code open source scanner, which is integrated to the automated audit in the release process, can identify all the components introduced in the code, match with the risk component rule, analyze insecure components, and form automated component vulnerability generation and force to fix vulnerabilities for specific development. At the same time, its vulnerability database is updated in real time from mainstream vulnerability disclosure websites.

ID	Vulnerability name	grade	CVSS	Components	Impact version	Details	Operating
1	Access Restriction Bypass	In danger	0	org.springframework.security:spring-security-core	[4.1.0, 4.1.5)[4.2.0, 4.2.4)[5.0, 5.0.3)	<a href="#">View</a>	<a href="#">Delete</a>
3	Access Restriction Bypass	High risk	0	org.springframework:spring-core	[5.0.5, 5.0.6)	<a href="#">View</a>	<a href="#">Delete</a>
4	Information Exposure	In danger	0	org.ovirt.engine.com:vdibroker	[4.1.4, 4.1.9)	<a href="#">View</a>	<a href="#">Delete</a>
5	Access Restriction Bypass	In danger	0	org.keycloak:keycloak-model-infinispan	[2.4.0.Final)	<a href="#">View</a>	<a href="#">Delete</a>
6	Signature Validation Bypass	High risk	0	com.inversoft: prime-jwt	[1.3.0)	<a href="#">View</a>	<a href="#">Delete</a>
7	Cross-site Scripting (XSS)	In danger	0	com.googlecode.wicket-jquery-ui:wicket-kendo-ui	[6.0.0.6.28.1), [7.0.0.7.9.2), [8.0.0-M0.8.0.0-M8.1)	<a href="#">View</a>	<a href="#">Delete</a>
8	Cross-site Scripting (XSS)	In danger	0	com.googlecode.wicket-jquery-ui:wicket-jquery-ui-plugins	[6.0.0.6.28.1), [7.0.0.7.9.2), [8.0.0-M0.8.0.0-M8.1)	<a href="#">View</a>	<a href="#">Delete</a>
9	Directory Traversal	High risk	0	org.apache.odr: odr-axis2	[1.3.3)	<a href="#">View</a>	<a href="#">Delete</a>
10	Directory Traversal	High risk	0	com.sparkjava: spark-core	[2.7.2)	<a href="#">View</a>	<a href="#">Delete</a>
12	Cross-site Scripting (XSS)	In danger	0	org.primefaces: primefaces	[6.2)	<a href="#">View</a>	<a href="#">Delete</a>

Tuya has strict specifications for the use and management of source code, and comprehensive matrix assessment are made through the evaluation of functions, popularity, development community activity, document perfection, and license evaluation. At the same time, conduct necessary use approval, testing and security audits. In particular, Tuya has strict risk profile for license compliance and prohibits the introduction of compliance risks.

## 8.2.4 Blackbox Scanning

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.

## 8.2.5 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.

## 8.2.6 IAST (interactive application security testing)

IAST (Interactive Scan) technology is a real-time dynamic interactive vulnerability detection technology. By combining all RASP node clients in Tuya service, it collects and monitors the runtime function execution and data transmission of the Web application, and conducts real-time real-time communication with the scanner. Interactively, efficiently and accurately identify security vulnerabilities.

### 8.2.7 Security Scanning on the Deployment Environment

For the application deployment environment, including ports, domain names, servers, and corresponding images, Tuya will conduct baseline security audits and use tools for continuous baseline security monitoring, including unsafe configurations, version vulnerabilities, baselines under compliance requirements, etc., and project-aligned at the same time, the release not only ensures the quality of the code itself, but also ensures the security of the deployment environment.

## 8.3 Security Test, Fixing and Verification

### 8.3.1 Security 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.

Tuya's penetration test follows the industry standards, references include OWASP top10, OWASP mobile top10, EN 303645 OWASP Top10 Privacy Risks Project, etc.

### 8.3.2 Security Vulnerability and Security Assessment Report

For the release phase, a system can only be released to the online environment after it passes the security test, fix all medium and high risk vulnerabilities, 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.

Safety report	title	version	Report name	founder	Creation time	operating
Vulnerability list	IOT platform security test	Product transfer function	IOT platform product transfer functional safety test	Tian Ji (Lu Feng)	2020-09-28 20:07:21	<a href="#">Send report</a>
List of new vulnerabilities	Jike Zhizhu APP	1.0.0	Jike Zhizhu APP Security Test Report	Chinese fir (Li Rongsheng)	2020-09-28 10:55:37	<a href="#">Send report</a>
My loophole	IOT platform security test	Procurement v1.32	IOT platform procurement module cross-category delivery requirements safety test report	Tian Ji (Lu Feng)	2020-09-27 15:32:53	<a href="#">Send report</a>
Repair follow-up	Smart community saas	Intelligent ladder control	Smart community safety test before the smart elevator control function goes online	Tian Ji (Lu Feng)	2020-09-27 15:26:05	<a href="#">Send report</a>
	Smart Home Light Environment APP	2.0.0	Smart home light environment APP safety test report	Chinese fir (Li Rongsheng)	2020-09-27 14:48:39	<a href="#">Send report</a>
	Hotel SaaS	Door lock management	Hotel SaaS door lock management function security test report	Chinese fir (Li Rongsheng)	2020-09-27 11:53:42	<a href="#">Send report</a>
	Smart community saas	V1.21 Fire protection legacy issues	Smart community saas V1.21 fire protection legacy safety test	Tian Ji (Lu Feng)	2020-09-26 17:58:31	<a href="#">Send report</a>
	IOT platform security test	Cloud Development 3.3	IOT platform cloud development platform 3.3 requirements security test before going online	Tian Ji (Lu Feng)	2020-09-26 15:54:24	<a href="#">Send report</a>
	Wisdom Apartment saas	Construction Housing-Construction Template	Apartment saas construction housing and construction template safety test report	Tian Ji (Lu Feng)	2020-09-25 16:59:36	<a href="#">Send report</a>
	IOT platform security test	Automatic firmware upgrade	IOT platform firmware automatic upgrade function safety test report	Tian Ji (Lu Feng)	2020-09-25 16:25:19	<a href="#">Send report</a>

## 9. Security Operation and Maintenance

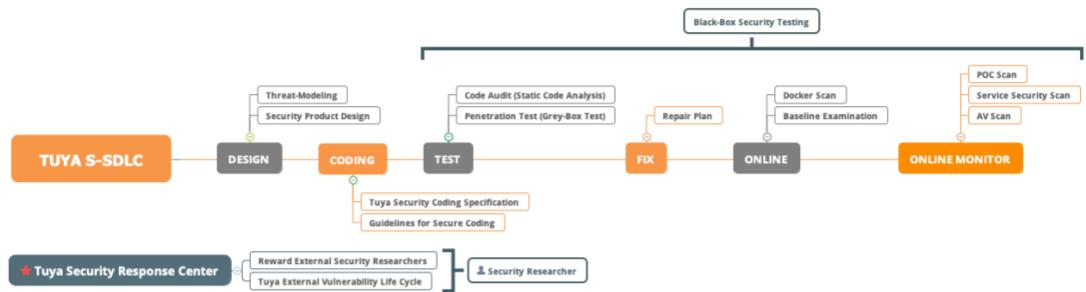
Unified management is carried out through Tuya's security operation & management platform; and strict access control and monitoring audit are implemented to ensure the O&M security.

- 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 IT infrastructure as a whole.

Tuya supports external white hats to submit vulnerabilities through Tuya SRC (<https://src.tuya.com/>) or external security email contacts, and provides the submitter with a vulnerability bonus of up to \$100,000 for a single high-quality and high-risk vulnerability. Tuya will verify and evaluate the vulnerability internally and if it is indeed a vulnerability, it will track the vulnerability repair through a work order until it is completed, Tuya will report the entire process to the white hat.

The vulnerability scores are comprehensively rated in accordance with the technical requirements of attack, the scope of impact, 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 and the CVSS3.1 for internal vulnerability risk rating.

If the vulnerability involves the App and hardware, the fix timeline can be referenced with Tuya SLA.

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 Asset Management

Security risk management based on assets and versions. Ability to quickly identify asset risks.

Version ID	Asset type	Asset Name	Version name	Number of vulnerabilities
58618	app	db-dm	2	0

### 9.1.2 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 IAST real-time scanning.

### 9.1.3 Penetration Test

Penetration testing is a practical demonstration of possible attack scenarios, simulating hackers trying to bypass the security control in Tuya network and being able to obtain the highest authority in the system.

Tuya conducts at least one internal penetration test every year for Tuya staff, organizational structure and IT structure. The test content includes external network penetration, internal network penetration, social engineering, etc.

Meanwhile, the penetration test from the third party may conduct at least once a year, such penetration service is provided by the leading professional third-party organizations,

including NCC Group, Kaspersky Lab, VTrust etc, which would cover security assessment of Tuya cloud platforms, apps, and hardware products.

#### 9.1.4 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.

#### 9.1.5 Security Risk Assessment

In order to maintain the appropriate control objectives and methods under the premise of considering the balance of control costs and risks, and to remediate information security risks at an acceptable level, Tuya conducts a risk assessment at least once a year.

The evaluation process is to establish a global modeling view for Tuya's existing services, analyze the risk factors in the internal mechanism of the system itself, and discover abnormal and malicious behaviors in the interaction between the system and the external environment, so as to complete the system weakness analysis and security threats, and reduce and control potential or existing risks.

#### 9.1.6 Security Auditing

Tuya's security team will conduct audits on all security system platforms, tool access, configuration changes, and permission granting processes, and keep all audit records.

At the same time, a set of internal security auditing platform is built, which is connected to the primary internal management system, which can conduct unified audit of all employee access and operation logs, and guarantee the accuracy, completeness and non-repudiation of audit logs.

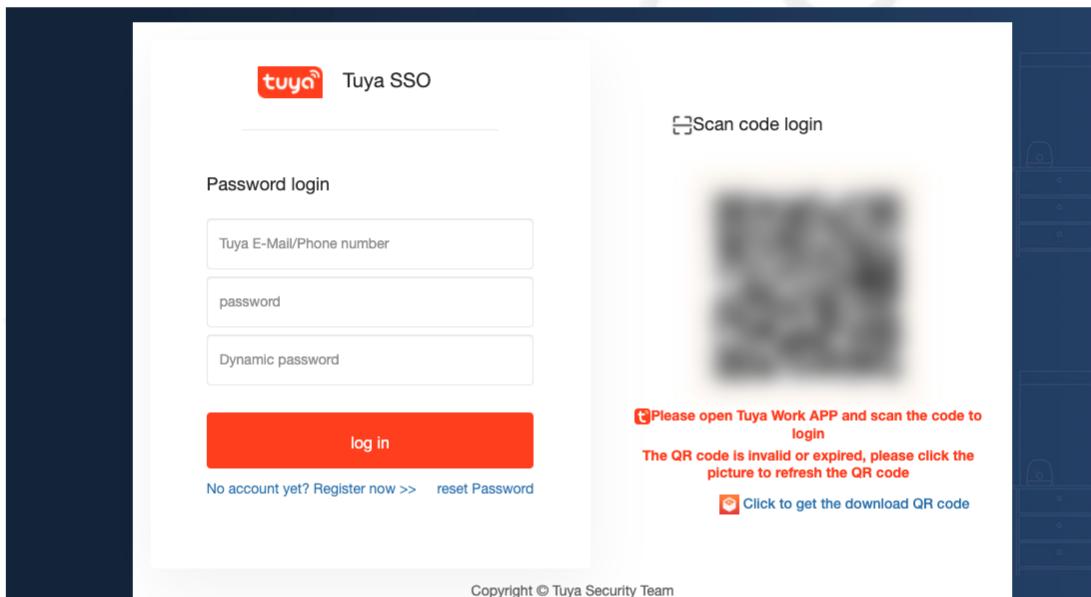
### 9.2 Access Control

Tuya implements unified management of system permissions, machine permissions, data permissions and other permissions of the IT system, and realizes a zero-trust permission management model. Based on the types of user identities, application identities, and application functions, it achieves minimal permission control.

#### 9.2.1 Authentication, Authorization, Accounting

The system permissions mainly include internal system platform permissions, application permissions, and machine permissions. The authorization of system permissions follows the "principle of minimum privilege", that is, to assign each authority role and only assign the "essential" authority needed to complete the task or operation. At the same time, the system strictly records all audit records for changes in permissions.

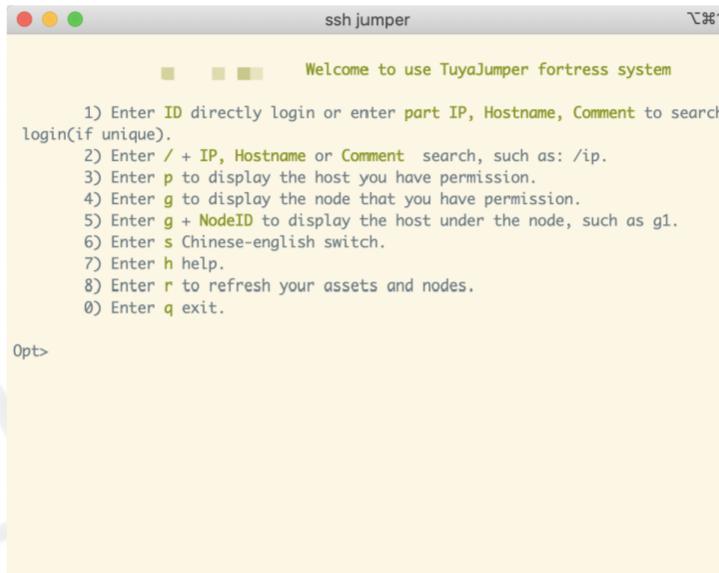
Regarding the identity authentication of the internal system, Tuya has implemented single sign-on (SSO) for all internal applications. At the same time, SSO realizes the ability of OTP. In addition to meeting all password management requirements, it also increases the dynamics of each login. Code verification capability.



Tuya has a unified authority management system (ACL) for the access verification of the internal system, which realizes the authorization of applications, application functions and data. There is a complete approval process management on the platform.

## 9.2.2 Access Control on Machines

Tuya employees have a unified management platform for machine permission application and approval. The approval of the corresponding supervisor, operation and maintenance, security and application person in charge is required to complete the authorization. After the employees are authorized, they can log in to the Jumpserver to control the limited access of the machine. At the same time, the authorization approval process, machine login session, command, file transfer, etc. have a complete audit process.



The screenshot shows the "Work Order Management" section of the Tuya Smart Platform. The left sidebar has a tree menu with categories like Home, Work order management, Resource management, Application management, Cost level, Fault management, Operation and maintenance, Process notification, Dispatch management, Role management, and Maven query. The main content area is titled "Access Request" and includes fields for applicant, application, permission (with dropdown options like "登录权限" and "Login permission"), reason, and a submit button.

### 9.2.3 Access Control on Applications

Tuya implements unified management and control of permissions for each application and calls between applications. The service access of Tuya's internal applications requires the use of a unified client component, through which the mutual identification of user identities and the control of permissions are realized. Application authentication is realized through a unified authentication service.

### 9.2.4 Access Control on Database

Tuya's database authority management mainly includes: application accounts, database platform accounts, etc. The application account refers to the account provided for the application to access the database, and the identity authentication is realized by identifying the machine where the application is located.

The accounts used by the database platform are specially created by the DBA, including read-write permission used to execute work orders and read-only accounts used by query modules. The database platform accounts are rotated every 3 months.

## 9.3 Security Management of Service Provider

### 9.3.1 the Risk Assessment of Service Provider

Tuya has formulated a screening mechanism and regular evaluation mechanism for platform software vendors. In addition to the security indicators of hardware products and the security standards of software services, Tuya needs to have a deeper understanding of the practices of various service providers in information security assessment and privacy compliance. The information security assessment involves security penetration testing and supplier security capability assessment. For details, please refer to Section 5.4.

### 9.3.2 the Monitoring of Service Provider

Real-time monitoring over the service quality, paying attention to the third parties security management, etc., so that Tuya can respond quickly when abnormalities occur.

## 9.4 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. Terminal Security

## 10.1 App

### 10.1.1 Client Program Protection

The security of the client is usually the first hurdle for hackers to breach. Taking the client as a black box, the attacker has to acquire the source code of the client and then 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 the 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 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.

### 10.1.2 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.

### 10.1.3 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. Secret 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.

### 10.1.4 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.

## 10.2 Hardware and Firmware Security

### 10.2.1 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.

### 10.2.2 Firmware Protection

Tuya has multiple protective approaches 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.

### 10.2.3 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.

#### 10.2.4 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.

#### 10.2.5 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.

## 11 Business Sustainability

### 11.1 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.

### 11.2 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.

### 11.3 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.

### 11.4 Emergency Drill

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

tuya.com

End of White Paper



©POWERED BY TUYA