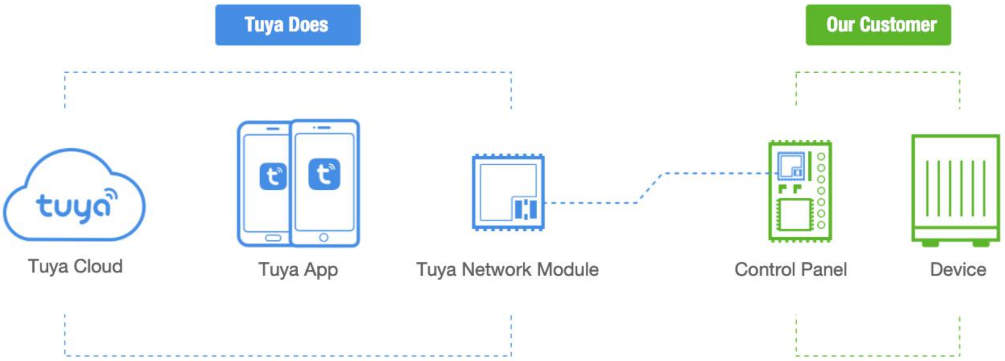
Tuya Smart White Paper on Information Security & Compliance

Version 5.2

Catalog

1. Introduction to Tuya Smart

Tuya Smart (NYSE: TUYA) is a global IoT development platform that builds interconnectivity standards to bridge the intelligent needs of brands, OEMs, developers, and retail chains across a broad range of smart devices and industries. Based on the global public cloud, Tuya connects different intelligent scenarios and smart devices by providing hardware development tools, integrating public cloud services, and offering an intelligent business development platform. Tuya provides comprehensive smart empowerment from technology to marketing to foster a neutral, open and accessible developer ecosystem.



1.1 Introduction to Tuya IoT PaaS

Based on the global public cloud, 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 high-availability (99.9%) computing services. 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 IoT PaaS 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

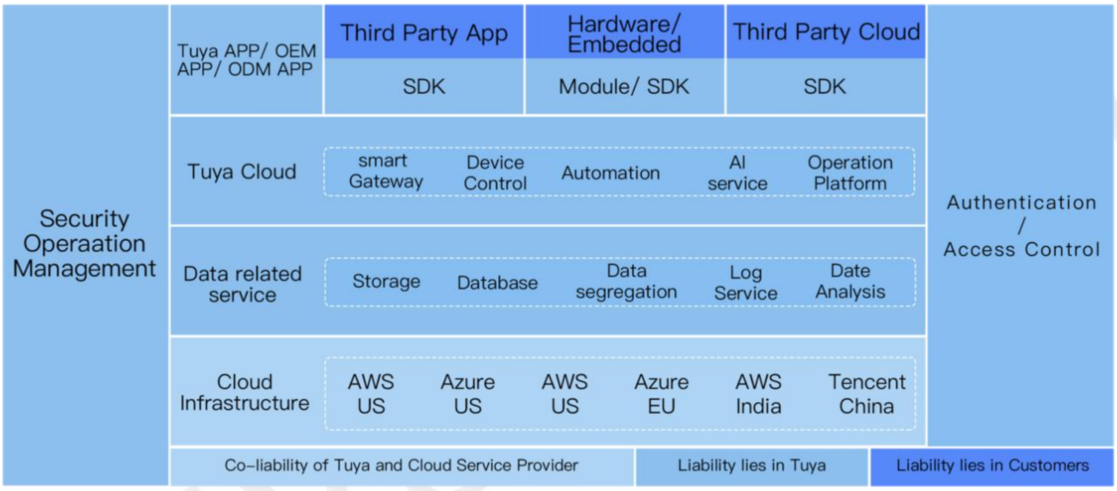
Tuya is devoted to providing customers with consistent, reliable, secure and conforming IoT access services, and guaranteeing the availability, confidentiality and integrity of the data of users. Tuya IoT PaaS's promise: Tuya IoT PaaS has data protection at its core and is built on cloud security. It 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 IoT PaaS.

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 IoT PaaS.

2. Security Responsibilities

Tuya is liable for security operation for services and data exchange on Tuya IoT PaaS 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 IoT PaaS, 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 IoT PaaS

Tuya IoT PaaS 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 IoT PaaS 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 IoT PaaS, practically protect its operation security, and guarantee the security of customer and user privacy. This omission mainly includes but is not limited to:

1) 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.

2) Access control management: resource and data access permission management, including user management, authority management, and identity authentication.

3) 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 Apps or Apps using Tuya-customized services, the customers will be responsible for privacy policies and compliance statements. The Tuya security & compliance team may provide assistance and advice on security solutions if necessary.

3. Compliance Endeavors

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

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

This is evidenced by the following compliance programs:

3.1 ISO/IEC 27001

Currently, Tuya has obtained ISO 27001 Information Security Management System

Certification (ISMS).

ISO/IEC 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:

1) Tuya establishes, implements, operates, monitors, reviews, maintains and improves information security with the methods based on business risk;

2) Tuya has set up a corresponding organization, established systematized security management system, and provided resource guarantee, to ensure information confidentiality, integrity and availability;

3) Tuya continuously improves information security management according to PDCA approach.

3.2 ISO/IEC 27017

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

ISO/IEC 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 IoT PaaS is set with special high-accuracy control system for cloud services.

3.3 ISO/IEC 27701

ISO/IEC 27701 is a privacy extension to ISO/IEC 27001 Information Security Management and ISO/IEC 27002 Security Controls. An international management system standard, it provides guidance on the protection of privacy, including how organizations should manage personal information, and assists in demonstrating compliance with privacy regulations around the world.

3.4 CSA STAR

Keeping IT networks and data secure is critical to Tuya's business. The need for more cost-effective storage and software solutions together with mobile access has led to a rise in the adoption of cloud computing – and while cloud computing has opened up many new opportunities. Through the implementation of CSA STAR Certification, in addition to a compliant ISO/IEC 27001 information security management system, Tuya ensures that we have a full understanding of the security risks involved and the business impacts. This allows Tuya to put controls in place to protect business critical information.

3.5 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.

3.6 EU GDPR Validation Program

The EU General Data Protection Regulation (GDPR) is intended to protect the fundamental privacy right of EU data subjects and the security of personal information. 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 though 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.

3.7 US CCPA Validation Program

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.

Tuya has obtained CCPA validation report issued by TrustArc. 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.

3.8 Enterprise Privacy Certificate (EPC)

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.

3.9 AICPA SOC2 Type II Audit

Standards promulgated by the American Institute of Certified Public Accountants, SOC2 Type II is a one of the authoritative audits in the field of data security, used to ensure that service providers manage data security, and protect corporate interests and the privacy of their customers. Tuya successfully obtains the SOC2 Audit Report to prove that Tuya has reached the leading level in protecting customer privacy and data security.

3.10 ETSI EN 303645 Certificate

ETSI EN 303645 is a European Standard on cyber security initiatives in consumer IoT security. This technical standard mainly regulates the cyber security of consumer IoT products and services, and commercial IoT products in the scope. It aims to establish a security baseline of defense for consumer IoT products and protect user privacy. It helps IoT products comply with security guidelines by design, and support global IoT product network security and European GDPR compliance. The related IoT law currently being promoted in the UK is also based on EN 303645 standard.

Product Service

Tuya Smart WBR3 (WIFI+BLE dual-mode) module has obtained TÜV SÜD’s ETSI EN 303645 evaluation and certification, indicating that Tuya’s WIFI and BLE security implementation in software and protocol have met the EU’s technical standards for consumer IoT security standards, it means more aligned with EU GDPR data protection regulation. Obtaining this certification indicates that Tuya's product line, including Tuya IoT PaaS, Tuya Smart Mobile Terminal, or Tuya Smart's modular products, have assessed by third-party endorsements with respect of GDPR regulation. In the future, Tuya Smart will continue to explore and develop safer products and services.

3.11 ioXt Product Security Certificate

ioXt validation is an authoritative global IoT security validation plan, and the only one driven by the industry participants. The ioXt Alliance is initiated jointly by technology and manufacturing conglomerates such as Google, Amazon, T-Mobile, Comcast. Products and Apps with ioXt SmartCert will definitely be a boost of confidence for consumers and retailers in this highly interconnected world.

ioXt

internet of secure things

Currently, Tuya holds ioXt certifications for 2 Apps and 9 types of modules; the 2 Apps being Tuya Smart and Smart Life, and the 9 modules being WBR3N, CB2L, CB2S, CB3L, CB3S, CBLC5, CBLC9, CBU and CBU-ipex.

3.12 More Compliance Efforts

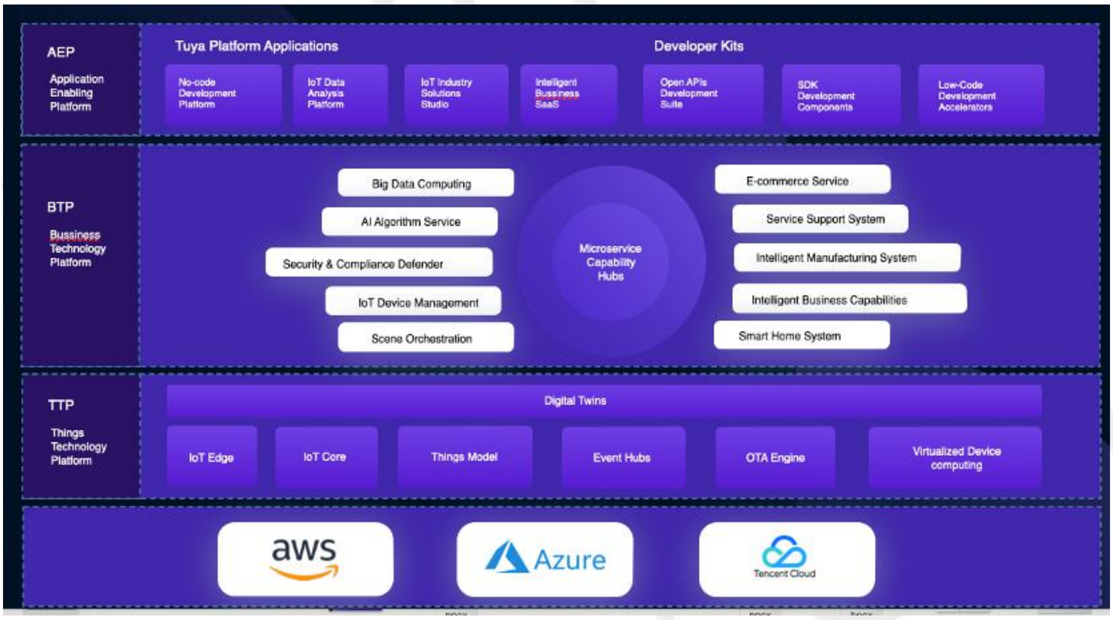
Tuya has a dedicated security and compliance team that closely tracks industry trends, and immediately respond to major global security and compliance standards, as well as data security and privacy regulations in various countries. Constantly, Tuya would cooperate with third-parties, technology consulting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

3.13 Regular Compliance Assessment and Auditing Efforts

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/IEC27701:2019, CSA STAR Cloud Security Certification, AICPA SOC2 Type II and other standards, and whether they meet the requirements of GDPR, CCPA and other relevant laws and regulations. In further to ensure effectiveness of the information security management system in accordance with industry high standards, and implement rectification and improvement based on the findings.

4. Tuya IoT PaaS Overview

4.1 Tuya IoT PaaS Infrastructure Architecture


AEP
Application Enabling Platform
Tuya Platform Applications
No-code Development Platform
IoT Data Analysis Platform
IoT Industry Solutions Studio
Intelligent Bussiness SaaS
Developer Kits
Open APIs Development Suite
SDK Development Components
Low-Code Development Accelerators
BTP
Bussiness Technology Platform
Big Data Computing
AI Algorithm Service
Security & Compliance Defender
IoT Device Management
Scene Orchestration
Microservice Capability Hubs
E-commerce Service
Service Support System
Intelligent Manufacturing System
Intelligent Business Capabilities
Smart Home System
TTP
Things Technology Platform
Digital Twins
IoT Edge
IoT Core
Things Model
Event Hubs
OTA Engine
Virtualized Device computing
aws
Azure
Tencent Cloud

TTP (Things Technology Platform) is a universal IoT connection and management platform that obtains abstract terminal data and capability model based on unified thing model, and accomplishes connection, authorization, authentication and management of the devices via IoT Core.

OTA Engine provides unified OTA strategy and data analysis, predicts when devices need upgrades, reduces device OTA risks, and optimizes device usage activities. Event Hubs provides flexible data relay and event subscription for the upper layer of the IoT Cloud, enriching modular micro-services of the upper layer competencies. According to various industry needs and differentiated competencies of the devices, Virtualized Device Computing enhances a smart device's hardware capabilities from the cloud platform by managing device access and scenes control through IoT Edge. These components enable the digital twins function that allows for real-time, closed-loop exchanges of data between the cloud and the physical smart devices throughout their life cycle, improves IoT deployment efficiency and helps developers optimize existing smart devices.

Business Technology Platform (BTP) is the competency center that provides the technology foundation to the upper layer of our Tuya IoT Cloud in the form of modular micro-services, offering competencies for Tuya IoT Platform and Developer Platform. The micro-services are interdependent and multiplex in standardized ways. We have conducted vertical divisions of service modules according to different business areas in an effort to make each modular micro-service as professional and standardized as possible in its own business area. For instance, the Smart Home System encompasses professional comprehension and integrated competencies from Tuya's years of experiences in the Smart Home vertical, which provides for industry competencies for home appliances, security systems, electricals and lighting, health and entertainment, as well as different vertical solutions for indoors and outdoors businesses. The upper layer applications, whether Tuya Platform Applications or Developer Kits, can all utilize competencies in the BTP.

Application Enabling Platform (AEP) includes Tuya Platform Applications and Developer Kits that allows us to deliver IoT PaaS, Industry SaaS and other value-added services. Tuya Platform, through no code development, industry solution development, big data analytics, and smart industry SaaS, forms a closed-loop application system that provides an all-platform business closed-loop foundation for the customers and instant ease of use for the developers. Developer Kits offers a comprehensive set of API, SDK and low-code development tools. The developers may add, customize or incorporate Tuya's competencies according to specific needs, without restrictions of industry or scenario, so that more efficient creation competencies are achieved by Tuya's low-code development tools.

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's 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.

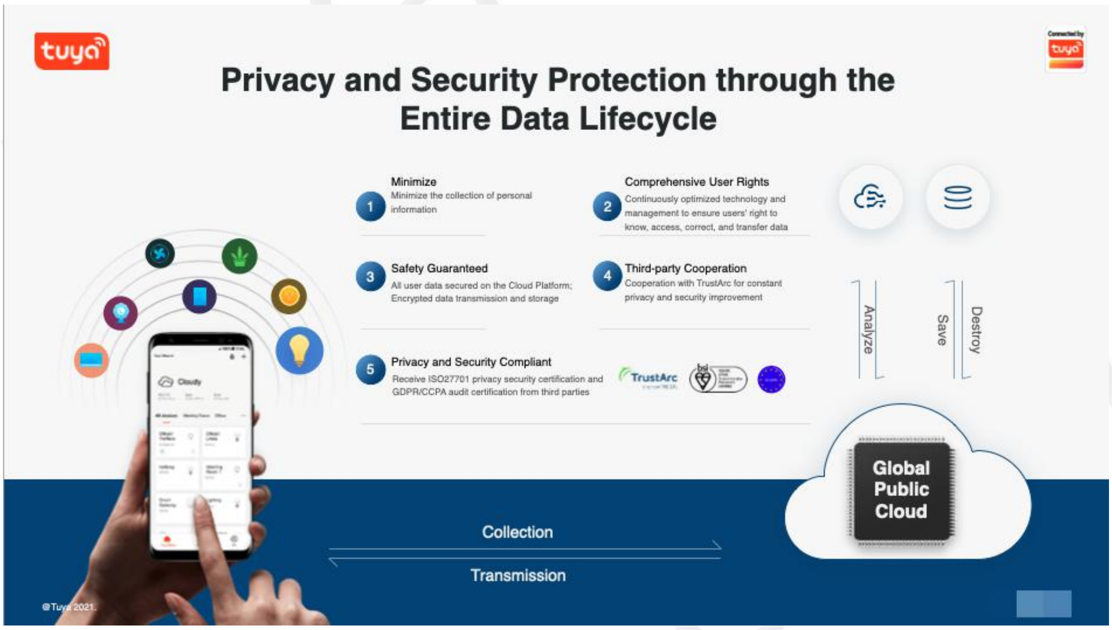
The cloud server providers currently under contract are Amazon, Azure, and Tencent Cloud.

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.



Privacy and Security Protection through the Entire Data Lifecycle

1 Minimize
Minimize the collection of personal information

2 Comprehensive User Rights
Continuously optimized technology and management to ensure users' right to know, access, correct, and transfer data

3 Safety Guaranteed
All user data secured on the Cloud Platform; Encrypted data transmission and storage

4 Third-party Cooperation
Cooperation with TrustArc for constant privacy and security improvement

5 Privacy and Security Compliant
Receive ISO27701 privacy security certification and GDPR/CCPA audit certification from third parties

5.2 Data Ownership

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 belong to individual users. Respectively, in the customized solution, the personal information 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 information, 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. Tuya, as the service provider, acts as a data processor that processes data per authorization of the customers. Tuya and the customers enter into stringent data processing agreements that provides for the scope and means of data processing, and relevant responsibilities and obligations. Tuya implements strict authorization and access control policies and corresponding technical safeguard structures to ensure that data is only accessed or processed under due authorization of the customers. Meanwhile, in order to guarantee data and privacy compliance, Tuya has deployed independent data nodes across the globe to execute localized data storage and processing, and implemented stringent data encryption mechanisms.

5.3 Data Security Lifecycle

5.3.1 The Fundamental Principles of Processing Personal Information

Any personal information processing activity by Tuya's products and services adhere to the principles of lawfulness, legitimacy, and necessity. Specifically, such data processing principles require the data controller/processor to act according to the following:

1) Consistency of rights and responsibilities (Accountability and Governance) – undertake liability for damages of the legitimate rights of the users caused by personal information processing activities.

2) Purposes limitation – identify lawful, legitimate, necessary and specific purposes for personal information processing.

3) Data subject authorization/consent – clearly state the purpose, means, scope and rules of personal information processing to the users, and obtain authorization/consent from such users.

4) Data minimization – unless otherwise agreed with the user, only process the minimum types and amounts of personal information to satisfy the authorized purpose of the users; not process, store, request, provide or transmit any data unrelated to the services; and timely delete personal information pursuant to agreement after completion of the purposes.

5) Transparency – publicly state the scope, purposes and rules of personal information processing in specific, understandable and reasonable manners, and accept external supervision of data processing activities.

6) Security safeguards – have security competencies commensurate to the security risks it faces, and implement sufficient management means and technical measures to ensure confidentiality, completeness and availability of personal information.

7) Subject engagement – provide means by which the users may access, rectify and

delete personal information, and ways to withdraw consent or cancel the account.

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 Individual 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 Policies for the Tuya Apps and websites.

✓ The Privacy Policy elaborates all personal information or the type of personal information being collected

✓ The Privacy Policy elaborates the source of such personal information and the purposes of processing.

✓ The Privacy Policy elaborates identities or types of third parties that may access the above personal information.

✓ The Privacy Policy may notify the users from time to time via email or in-App prompted notices. When any significant change has been made to, e.g., the way or purposes of processing personal information, or on the new type of data collection, a separate consent shall be made by the user.

◆ Cookie Statement on the website

✓ Displays all Cookies and their functions.

✓ Users may turn off functional and advertising cookies by one click, which will not affect functioning of the websites.

◆ Users’ withdrawal of consent

✓ Allows users to withdraw consent in using services of the App or the websites. After withdrawal, Tuya will not subsequently process any personal information of the user.

✓ In order to analyze usage conditions of Tuya’s products and services and to enhance user experience, Tuya may conduct data analytics of data provided and reported by the users and timely examine issues that the users may encounter when using the products. Users may turn off data analytics in the Tuya App.

✓ In order to provide customized products and tailored services for the users, Tuya may process account information, usage information and device information of the users. If a user does not consent to such processing, he/she may elect to turn off selection in the Privacy Settings in the App.

2) Right of Access

Users can access personal information 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 information associated with services and functions.

3) Right to Erasure

As the owner of the data, the user can cancel the account and delete user 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.

The user may request deletion of specific personal information when one of the following conditions is met:

◆ Personal information shall be removed per the user’s request, when:

✓ Tuya collects or uses personal information in violation of applicable law or regulation; or

✓ Tuya collects or uses personal information in violation of relevant agreement with the user.

◆ Tuya, in violation of applicable law or regulation or relevant agreement with the user, shares or transfers personal information to any third party; when the user requests deletion, Tuya shall immediately cease such sharing or transfer, and notify relevant third party to timely delete the personal information.

◆ Tuya, in violation of applicable law or regulation or relevant agreement with the user, publicly discloses personal information; when the user requests deletion, Tuya shall immediately cease such public disclosure, and notify relevant recipient to timely delete the personal information.

4) Right to Rectification

Users can manually and proactively rectify the personal information on the App if there is any incorrect or out-of-date information about the individual. In case the App does not provide the function to rectify certain information, the user may provide feedback in the Tuya App or contact customer service by email.

5) Right to Data Portability

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

5.3.3 Security Management during 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.

All data collection will undergo stringent risk and compliance review by the compliance team during demand assessment or planning design phase before officially initiating R&D process. Meanwhile, the compliance team will conduct DPIA from time to time to perform analytics on sensitive data, ensuring compliance of data collection with applicable laws.

2) Data Storage

◆ Data and File Storage

✓ Tuya IoT PaaS provides different data storage services under various business scenarios. Personal information is encrypted and stored using AES256, and personal sensitive data will be subject to extra AES encryption. Also, certain sensitive data will be desensitized when necessary. 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.

- The EU/EEA: Tuya has deployed two data centers in EU, the AWS Frankfurt, Germany, and Azure in Netherlands.

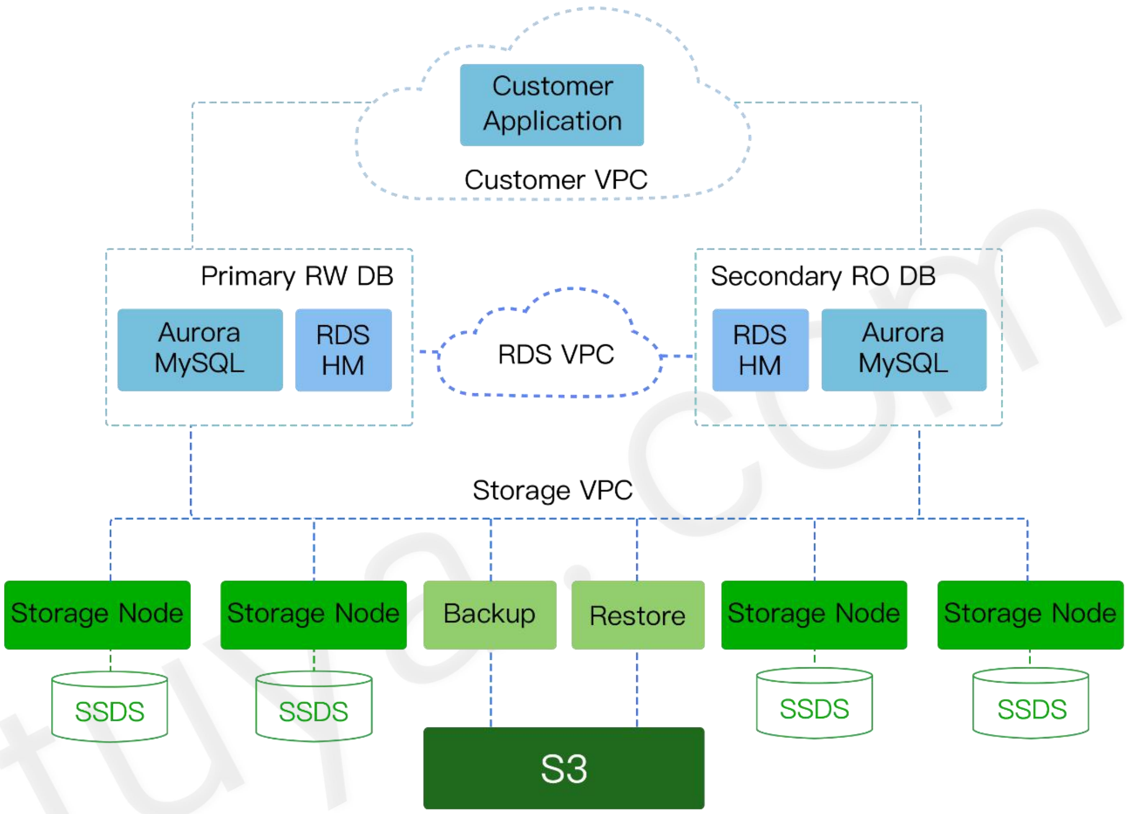
- India: The data is stored in a server center in Mumbai, India, and basic cloud computing support is provided by Amazon AWS.

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

Tuya implements strict data classification and handling policy internally to specify the scope of data property, identifying principles for classification and relevant persons in charge, and relevant requirements of data governance.

Tuya classifies data according to the source, content and purpose of data, and divides data into different sensitivity levels according to value of data, sensitivity of content, impact and scope of distribution.

◆ Access Control Mechanism

✓ Tuya IoT PaaS 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 IoT PaaS 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 another dashboard. Therefore, measures such as de-identification or desensitization have been adopted. Specific business scenarios require displaying personal information, 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 information, 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 information 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 information is limited to the user’s express consent so that the personal information 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 Technical Measures for Data Security and Privacy

1) Secured Transmission of Data

- The integrity of the data transmission

  When the application program processes the data transmission process, including without limitation, device-cloud communications, App-cloud communications, it will perform integrity check, usually using the HMAC-SHA256 algorithm.

- The desensitization and encryption of the data content

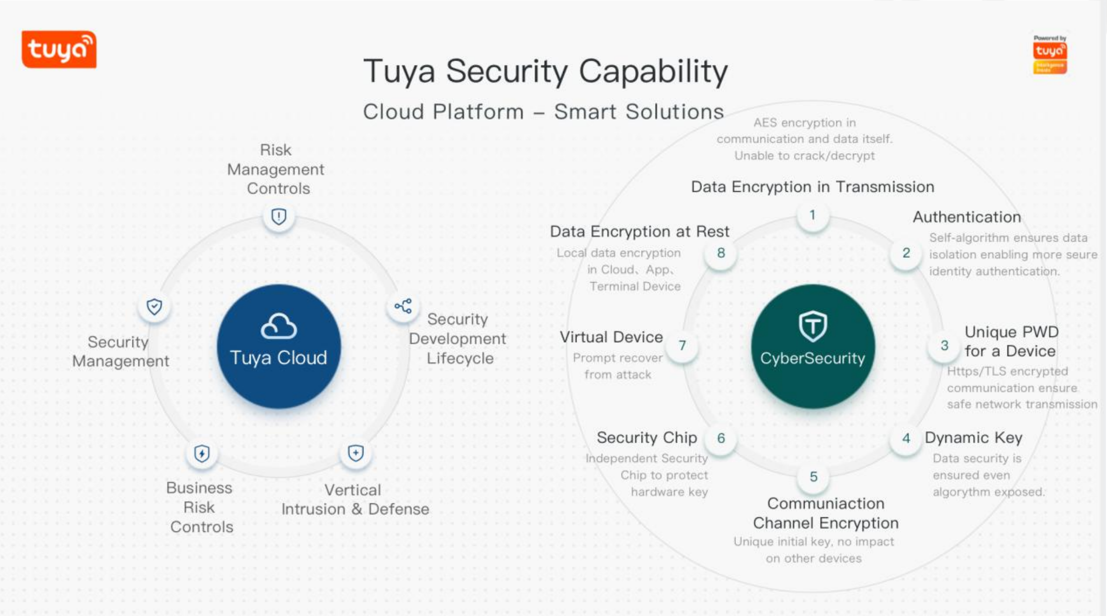
  AES-128 encryption is utilized in the communication between the APP and the cloud, the communication between the device and the cloud, the communication between the APP and the device, as well as the communication between the device and the device, the sensitive data, including passwords, biometric data, 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 IoT PaaS provides multiple security strategies to ensure the security of data generated by smart devices. As shown below:



Tuya Security Capability

Cloud Platform – Smart Solutions

Tuya Cloud

Risk Management Controls

Security Development Lifecycle

Vertical Intrusion & Defense

Business Risk Controls

Security Management

CyberSecurity

1 Data Encryption in Transmission

AES encryption in communication and data itself. Unable to crack/decrypt

2 Authentication

Self-algorithm ensures data isolation enabling more seure identity authentication.

3 Unique PWD for a Device

Https/TLS encrypted communication ensure safe network transmission

4 Dynamic Key

Data security is ensured even algorythm exposed.

5 Communiaction Channel Encryption

Unique initial key, no impact on other devices

6 Security Chip

Independent Security Chip to protect hardware key

7 Virtual Device

Prompt recover from attack

8 Data Encryption at Rest

Local data encryption in Cloud、App、Terminal Device

- ◆ 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 to ensure device security.

✓ Transmission encryption: TLS1.2 data encryption transmission protocol and mandatory authentication of certificates.

✓ 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 IoT PaaS can be found in Chapter 7.

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

5.3.5 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 information 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 information, clarifies the division of responsibilities, standardizes data processing procedures, regularly reviews access, and strengthens data security training.

5.3.6 Data Sharing Mechanism

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:

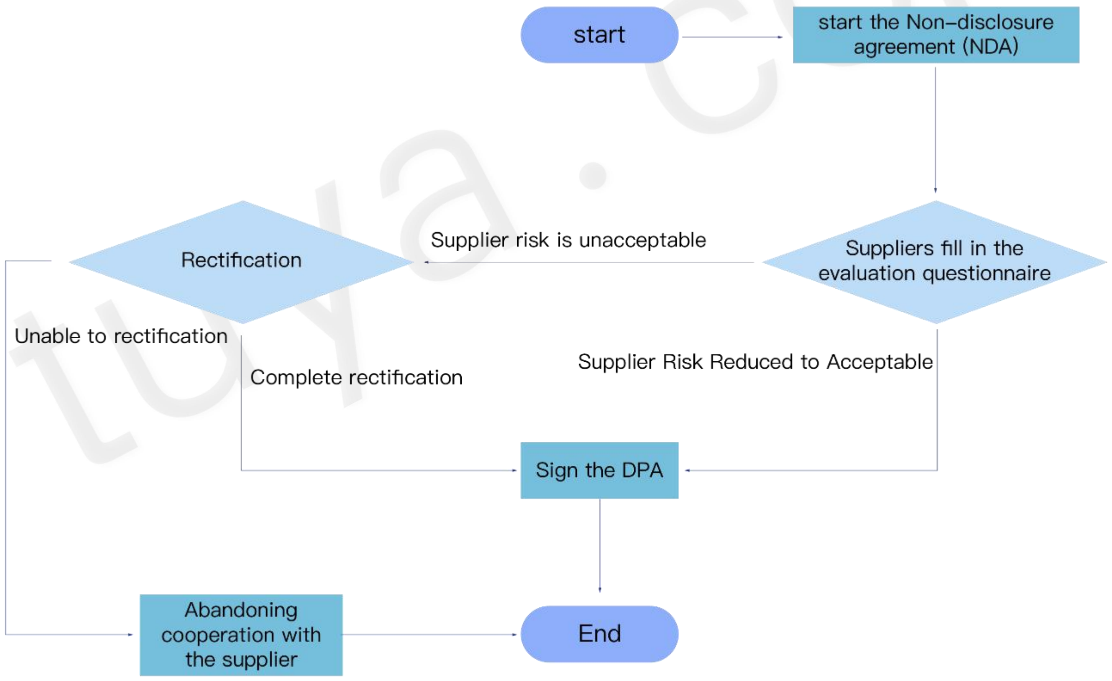
1) Third-party smart features, such as Google and AWS, require users to actively authorize their account data to be shared to the corresponding voice platform, so as to realize support for smart home scenes of Tuya platform users like Google Home, AWS Echo, etc.

2) 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 information, 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 "Third Party Risk Management" is implemented. The review generally includes relevant data protection regulations or security and privacy management requirements accordingly. The evaluation process is roughly shown as follows:



start
start the Non-disclosure agreement (NDA)
Suppliers fill in the evaluation questionnaire
Supplier risk is unacceptable
Rectification
Unable to rectification
Complete rectification
Supplier Risk Reduced to Acceptable
Sign the DPA
Abandoning cooperation with the supplier
End

With the help of 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 a 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.

6. Security and Compliance 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 resource 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 and privacy team, which is composed of the former members from renowned domestic and international Internet companies and conventional security manufacturers. 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 Compliance Committee

Tuya has established a 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 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 employee’s act is 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 and Compliance 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 quarterly security awareness assessments and education required for all employees will be conducted 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.

Tuya Security team will at times conduct internal security defense tests on quarterly basis, and will issue corporate-wide reports on employees failing such tests.

6.5 Security and Compliance Training

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 Security and Compliance 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. Such training sessions include without limitation, secure coding rules training, penetration test skills training, typical security vulnerability training, and business security training.

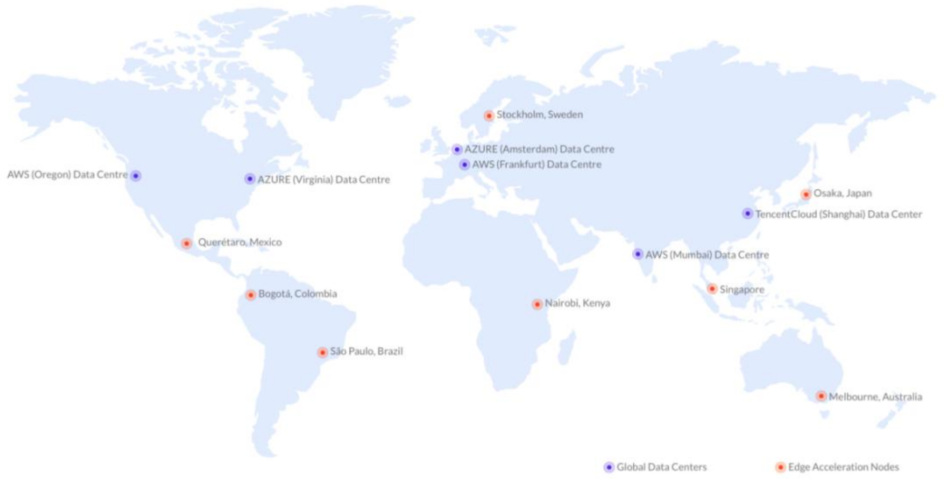
7. Security Assurance of IoT PaaS

7.1 Physical Security

As an IoT cloud computing service provider, Tuya IoT PaaS makes efforts to provide each customer with secure, stable, sustainable and reliable physical infrastructure. Tuya IoT PaaS 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 IoT PaaS 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 IoT PaaS 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; 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).

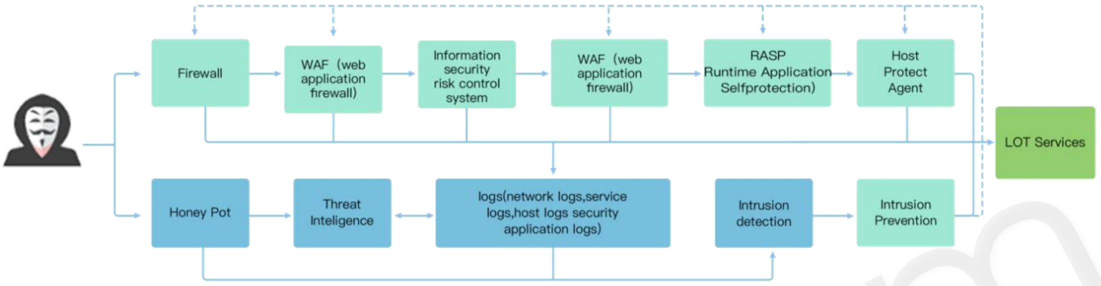
Tuya IoT PaaS deploys data and systems flexibly in different data centers or different regions to meet disaster recovery requirements for businesses. Tuya IoT PaaS allows customers to designate location of data storage to the extent permitted by applicable laws.

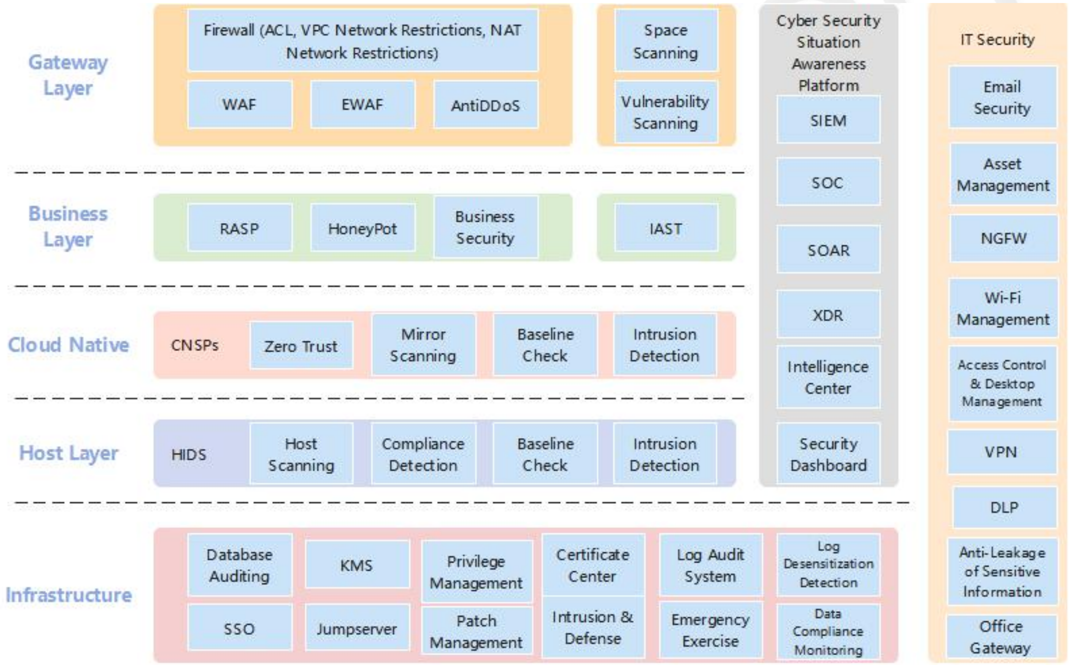
7.2 Network Security

7.2.1 Security Architecture

Tuya IoT PaaS has mature in-depth network security defense architecture, including Web Application Firewall (WAF), security incident analytics platform, Runtime Application Self-Protection (RASP)，Cloud Native Security Platforms (CNSPs), Hose-based Intrusion Detection System (HIDS), HoneyPot, and multiple protection mechanisms to identify and respond to the threats from the Internet on technical structure level in multi- layer and multi-dimension ways.

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


Firewall
WAF (web application firewall)
Information security risk control system
WAF (web application firewall)
RASP Runtime Application Selfprotection)
Host Protect Agent
LOT Services
Honey Pot
Threat Inteligence
logs(network logs,service logs,host logs security application logs)
Intrusion detection
Intrusion Prevention



7.2.2 Network Communication Security

All communications of current smart hardware solutions on Tuya IoT PaaS 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 IoT PaaS 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.

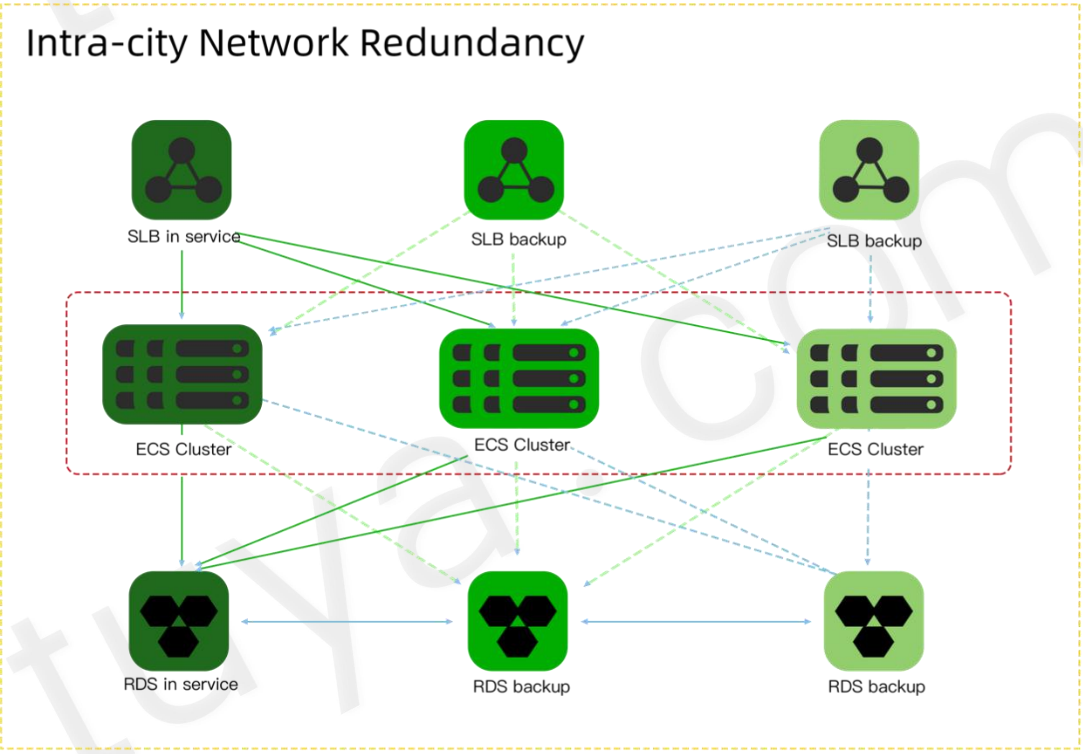
With regards to the network access isolation for cloud users, Tuya provides multiple security mechanisms including virtual-control-level resource access control policy, inter-private network isolation policy in cloud platform, Web console permission distribution and authentication, interface conversation 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 IoT PaaS 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 IoT PaaS's self-built anti-DDoS high imitation cluster can intercept DDoS attacks of certain traffic, including IP address scanning at the network layer, malformed packet attacks, and fragmentation attacks; it can identify and intercept common TCP Flood and

UDP Flood at the transport layer, launch amplification attacks, TCP/UDP fragmented packet attacks, malformed packet attacks, DNS poisoning, etc.; and identify and intercept application layer CC attacks, HTTP slow attacks, SSL DDoS attacks, SIP Flood and MQTT connections attacks as well.

In the meanwhile, in order to sustain service stability, Tuya has also enabled the DDoS protection function of cloud platforms such as AWS and Microsoft Azure to protect all data centers, with automatic detection, scheduling and cleaning capabilities.

In terms of CC attack (Challenge Collaspsar), Tuya would implement firewall and WAF, to a certain degree, restricting and blocking of abnormal connections. Meanwhile, checking 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, as well as HoneyPot detectors and services for external networks, 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.

7.3.2 Internet Intrusion Prevention:

Intrusion blocking is performed through security protection tools such as network firewall, WEB application firewall (WAF), and Runtime Application Self-Protection (RASP) and Cloud Native Security Platform.

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

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.

7.3.3 Host Security Detection

Host computer supervision: including WEBSHELL detection, under which servers are provided with webshell real-time detection engine to enable real-time detection, deletion and reporting to webshell; and host computer abnormal login detection, insecure baseline configuration detection, host computer vulnerability detection etc.

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 IoT PaaS 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.

To adapt to the various needs of the customers for account security, the customer may define its own secure password policy, including without limitation, customized App password complexity level to be set up in backstage.

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.

Meanwhile, on content compliance level, the content compliance audit engine can identify potentially unsettling, insecure or inappropriate contents, which can effectively reduce risks of content violation and filter harmful information. It can also substantially filter any content in violation of national laws, regulations and policies, including pornographic contents (obscene or vulgar information), violence related contents (weapons, arms, terrorism, gruesome graphics), and political contents (sensitive/insensitive figures).

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 through zero-contact certificates by code deployment, 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.

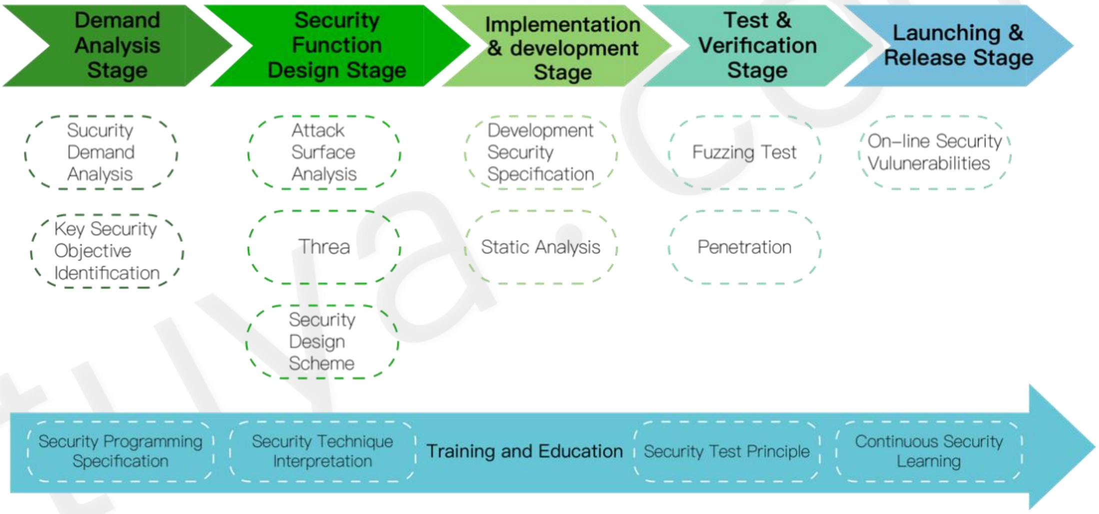
7.4.6 Configuration Management

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.


Demand Analysis Stage
Security Function Design Stage
Implementation & development Stage
Test & Verification Stage
Launching & Release Stage
Sucurity Demand Analysis
Key Security Objective Identification
Attack Surface Analysis
Threa
Security Design Scheme
Development Security Specification
Static Analysis
Fuzzing Test
Penetration
On–line Security Vulunerabilities
Security Programming Specification
Security Technique Interpretation
Training and Education
Security Test Principle
Continuous Security Learning

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 and 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 kits for the developer, and require the developer to undergo training related to secure coding standard, provide R&D engineers with automatic detection tools and test cases in order to minimize security risks before submission for testing. Meanwhile, upon completion of each code submission by R&D, automated code audit and open source component audit will be carried out, and in case of risks, the corresponding developer will be noticed immediately 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

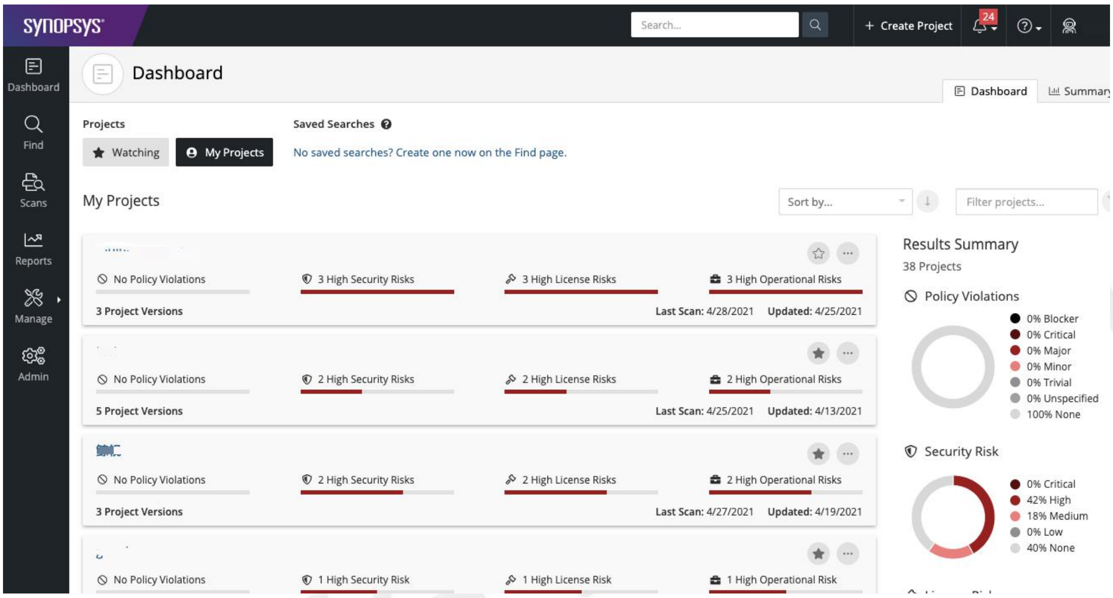
The code auditing independently developed by Tuya is able to accurately locate the high-risk function entry by means of the syntax tree analysis, and do retrograde analysis before use of the function, in order to discover the unsecure uses. Meanwhile, prevailing vulnerability information will be tracked 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.

At the same time, Tuya also integrates the international mainstream third-party code audit tool, which supports Tuya's main languages (including without limitation, JAVA, C/C++, Python, NodeJS) through this tool, which can effectively help the business to find vulnerabilities.

8.2.3 Open Source Auditing

Tuya security team deployed Blackduck, the best solution for open source audits from both oversea and domestic markets, which connected the multi-terminal CICD to perform security checks before code release and third-party SDK or binary firmware packages.

Blackduck can identify and track the open source components of applications and containers, can detect and assist in the development and repair of open source vulnerabilities, and it can verify and comply with the terms of the open source license. Through Blackduck's products and professional security team behind the project, it can ensure that the internal business can locate the security vulnerability of open source formation or supply chain in the first time.



Dashboard

No saved searches? Create one now on the Find page.

My Projects

No Policy Violations | 3 High Security Risks | 3 High License Risks | 3 High Operational Risks
3 Project Versions | Last Scan: 4/28/2021 | Updated: 4/25/2021

No Policy Violations | 2 High Security Risks | 2 High License Risks | 2 High Operational Risks
5 Project Versions | Last Scan: 4/25/2021 | Updated: 4/13/2021

No Policy Violations | 2 High Security Risks | 2 High License Risks | 2 High Operational Risks
3 Project Versions | Last Scan: 4/27/2021 | Updated: 4/19/2021

No Policy Violations | 1 High Security Risk | 1 High License Risk | 1 High Operational Risk

Results Summary
38 Projects

Policy Violations
- 0% Blocker
- 0% Critical
- 0% Major
- 0% Minor
- 0% Trivial
- 0% Unspecified
- 100% None

Security Risk
- 0% Critical
- 42% High
- 18% Medium
- 0% Low
- 40% None

Besides the Blackduck deployment, Tuya has self-developed open source scanning tools as supplement, which was integrated to the auto-auditing in release process to identify all the component introduced in the code, match it with the risk component rule base, analyze insecure components, and generate automated vulnerability and push it to the designated developer for repair, in the meantime, the vulnerability repository is updated in real time from mainstream vulnerability websites public to all.

Tuya has strict specifications for the use and management of source code, and comprehensive matrix assessment are made through the evaluation by Blackduck, on 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 WEB Vulnerability 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 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.

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.

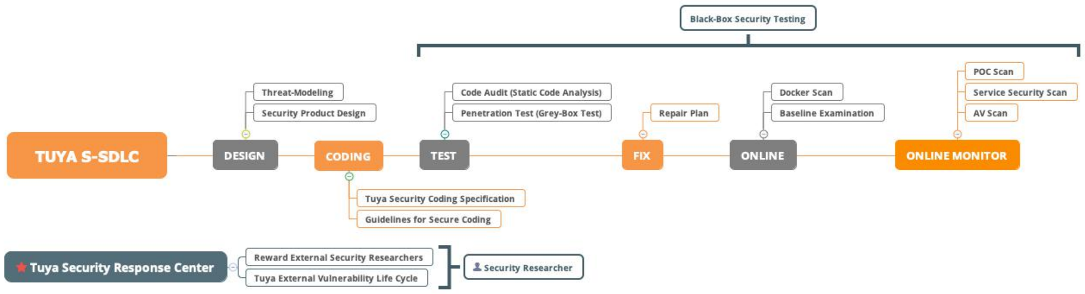
- Authorization: based on the position and role, Tuya's employees are granted the limited resource access rights as per the principle of the least privilege and the separation of duties. The employees may apply for various access rights from the centralized authorization management platform according 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 IoT PaaS 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 IoT PaaS 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.


Black-Box Security Testing
TUYA S-SDLC
DESIGN
Threat-Modeling
Security Product Design
CODING
Tuya Security Coding Specification
Guidelines for Secure Coding
TEST
Code Audit (Static Code Analysis)
Penetration Test (Grey-Box Test)
FIX
Repair Plan
ONLINE
Docker Scan
Baseline Examination
ONLINE MONITOR
POC Scan
Service Security Scan
AV Scan
Tuya Security Response Center
Reward External Security Researchers
Tuya External Vulnerability Life Cycle
Security Researcher

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.

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. In 2021, the leading professional third-party organizations have provided penetration services for Tuya, including Rapid7, wizlynx group, UnderDefense, ScienceSoft, VTrust etc., which would cover security assessment of Tuya IoT PaaS, Apps, and hardware products.

In addition, Tuya releases Bug Bounty through SRC (official website: https://src.tuya.com). Tuya also interfaces with a third-party public testing platform, aiming to enable global white hats to report security vulnerabilities of Tuya products and services through afore-mentioned channel.

9.1.4 Security Incident Response

Tuya has established and improved its internal network security incident emergency work mechanism to improve its ability to respond to emergent network security incidents, prevent and reduce the loss and harm caused by network security incidents, improve emergency response capabilities, and ensure the safe operation of the company's business.

The security incident response process adopts strict classification of security incidents and vulnerabilities. In response to incidents, the corresponding processing and execution procedures are carried out according to the classification, including incident discovery, detection, suppression and eradication recovery, and follow-up summary of the entire incident life cycle.

In accordance with the policy of "active prevention, timely detection, rapid response, and ensured recovery", the below flowchart is followed in the management of security incidents. The sequence of process flow follows the direction of the arrow. The purple lines in the figure represents the "top-down" situation, which mainly represent the processing procedures triggered by the higher-level security department, with relevant security report as the entry point; the blue lines in the figure represent "bottom-up" situation which mainly refers to the processing procedures triggered by the monitor or system maintenance team, with the discovery of the incident by the security monitoring or information security operation maintainer. The brown lines in the figure represents the situation of entering the "non-emergency security incident processing process", which mainly represents the processing procedures triggered by the security monitoring personnel. Tuya may also provide 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 Audit

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.

SSO: 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.

ACL: 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.

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 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 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 IoT PaaS is able to provide customers with 24x7 technical support on cloud services.

10. Terminal Security

10.1 Mobile 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.

Meanwhile, most App’s security enhancement function supports customer to manually turn on or configure it on the Tuya IoT Platform backstage.

10.1.2 Communication Security

App-cloud communication channels include protocols such as HTTPS and MQTT over TLS, which all adopt TLS1.2 security protocol for communications to perform strict certificate information authentication to avoid risk of hijack. Customer may turn on SSL Pinning on the Tuya IoT Platform backstage; the default setting is on when exporting the App.

Data transmitted via App-cloud communications are all encrypted using AES128. The encryption key is a random dynamic encryption key generated based on each customer’s dialogues, and is only valid for the current dialogue, which sufficiently protects data security during transmission.

10.1.3 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.

10.1.4 Data Security

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

1) Internal storage:

◆ 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.

◆ SQLite database: it does not store user-related sensitive information.

◆ SharedPreferences configuration file of Android: no sensitive information is allowed.

2) System log: no interactive logcat or log file can be printed or saved at any formal client.

3) Secrete key chain data: important Key cannot be hard coded, and save the key with a self-developed security algorithm.

4) Memory data: user data will not be saved in the memory during important operation.

10.1.5 Privacy and Compliance on App

Tuya's client terminal implements national laws and regulations and global mainstream information security and privacy protection regulations, and has a complete user personal information protection program, including but not limited to public collection and use rules, complete procedures to ensure strict implementation of the principle of necessity, and express collection The purpose, method and scope of the use of personal information, complete user consent solutions, detailed complaints, reports, or manual processing channels for user feedback, can be seen in Chapter 5.

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) 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 lawfulness of the firmware and that it 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 Exercise

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

End of White Paper