Tuya Smart White Paper on Information Security & Compliance

Version 6.0

Legal Statement

Tuya Smart kindly reminds you to thoroughly read and fully understand all clauses in this legal disclosure before proceeding with the reading or use of this document. If you have read or used this document, your actions will be deemed as acceptance of all the contents of this statement.

【Copyright and Trademark Statement】

1. You are required to download and obtain this document only through Tuya's official website or other authorized channels provided by Tuya, and it should only be used for your own lawful and compliant business activities. The contents of this document are considered confidential information of Tuya Smart, and you are obligated to strictly adhere to confidentiality; without the prior written consent of Tuya, you may not disclose the contents of this manual to any third party or provide it for their use.

2. All content in Tuya's documents, including but not limited to images, architectural designs, page layouts, and textual descriptions, are legally owned by Tuya and its affiliates, who possess all relevant intellectual property rights, including trademarks, patents, copyrights, and trade secrets. Without the written consent of Tuya and its affiliates, no one is allowed to use, modify, copy, publicly disseminate, adapt, distribute, or publish the content of Tuya's website, product programs, or content. Furthermore, no individual is permitted to use, disclose, or replicate Tuya's name (including, but not limited to, brands associated with Tuya and its affiliates such as "Tuya Smart") for any marketing, advertising, promotional, or other purposes without Tuya's prior written agreement. This prohibition extends to any prominent symbols, logos, or similar business names, trade names, trademarks, product or service names, domain names, visual symbols, emblems, or identifiers that may enable third parties to recognize Tuya and/or its affiliates.

3. No entity is allowed to duplicate, modify, plagiarize, or disseminate any part of this document without Tuya's prior written consent. Additionally, this document does not

confer any legal rights related to the intellectual property of Tuya products. You are permitted to copy and use the content of this document solely as internal reference material.

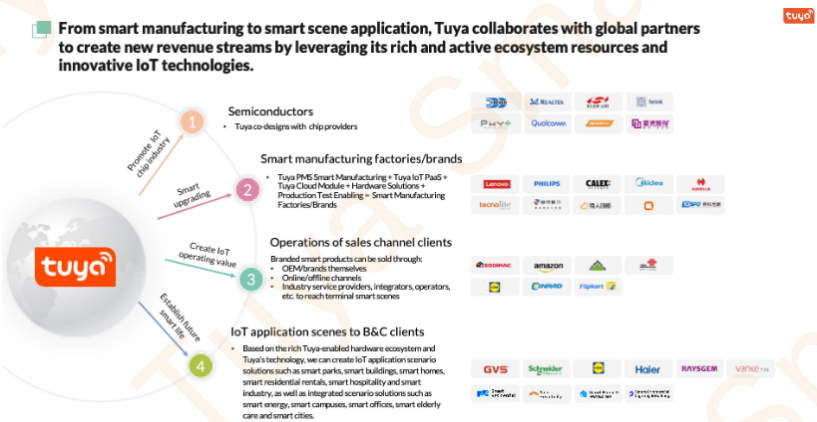
【Important Considerations】

1. The products, services, or features you have purchased are subject to the commercial agreements and terms of Tuya Smart. The entire or part of the products, services, or features described in this document might not fall under your purchase or usage scope. Unless there is a stipulation in the contract, Tuya provides no explicit or implicit statement or warranties about this document.
2. The content of this document may change to reflect product updates, tweaks, or other reasons. Tuya reserves the right to modify this document's contents without prior notice, and periodically posts updated user documents on Tuya's authorized channels. You're encouraged to keep abreast of the user document versions and download or retrieve the most recent version via Tuya's authorized channels.
3. This document is meant to serve as a reference guide for users when using Tuya's solutions, products, and services. Tuya provides this document based on the current "as is" condition of products and services which may have flaws or limited functionality. Tuya gives the maximum effort to provide respective introductions and operational guides based on current technology. However, Tuya expressly declines all explicit or implicit warranties regarding the accuracy, completeness, reliability, and applicability of this document's content. Neither Tuya nor those associated with it can be held legally responsible for any errors, financial losses, or damages suffered by any entity, company, or individual who downloaded, used, or relied on this document. In no circumstance will Tuya bear responsibility for any indirect, consequential, punitive, incidental, special, or penal damages, including profit losses experienced by users relying on this document (even if Tuya was made aware of such possible losses).
4. If you find any discrepancies or errors in this document, please contact Tuya Smart directly. We will address and resolve it at the earliest.

Content

1. Introduction of Tuya Smart

Tuya Inc. (NYSE: TUYA; HKEX: 2391) is a global leading cloud platform service provider with a mission to build a smart solutions developer ecosystem and enable everything to be smart. Tuya has pioneered a purpose-built cloud developer platform with cloud and generative AI capabilities that delivers a full suite of offerings, including Platform-as-a-Service, or PaaS, Software-as-a-Service, or SaaS, and smart solutions for developers of smart device, commercial applications, and industries. Through its cloud developer platform, Tuya has activated a vibrant global developer community of brands, OEMs, AI Agents, system integrators and independent software vendors to collectively strive for smart solutions ecosystem embodying the principles of green and low-carbon, security, high efficiency, agility, and openness.



1.1. The Mission of Information Security Assurance

Tuya is committed to delivering consistent, reliable, secure, and compliant IoT access services to customers, thereby effectively guaranteeing the availability, confidentiality, and integrity of data for both customers and their users. With data protection as our core focus and cloud security capabilities serving as the cornerstone, Tuya leverages its exclusive IoT solutions to establish industry-leading competitiveness, build a comprehensive security assurance system for its cloud platform, and steadfastly

considers information security as one of the key developmental strategies of Tuya Cloud. To accomplish these goals, Tuya has implemented security measures at various levels, encompassing security checks, defenses, as well as monitoring and auditing of all external services. This forms a comprehensive protective process that covers pre-event, during-event, and post-event stages. Additionally, by establishing a complete security system for software and hardware research and development, Tuya seamlessly integrates information security and compliance assurance throughout the entire software development and project management lifecycle, ultimately ensuring the safety and quality of the delivered hardware and software products.

1.2. Strategy for Security Compliance

As a tech company specializing in AI+IoT, Tuya Smart attaches great importance to security and compliance matters. Tuya's strategy for security compliance incorporates various measures designed to ensure our products and services can optimally meet security and compliance standards and requirements across different regions.

First, Tuya has a dedicated information security team responsible for monitoring and protecting our networks and systems from threats like cyberattacks and data breaches. We also routinely subject our products and services to security testing and vulnerability scanning, alongside strengthening measures such as data encryption and access control.

Furthermore, we abide by all relevant laws, regulations, and standards, including data protection and cybersecurity laws. Based on these provisions, we have crafted internal guidelines and operational procedures to ensure our business operations align with all legal requirements and norms.

Finally, with an eye on emerging security and compliance technologies, we aim to continually update and refine our strategy for security compliance to handle ever-evolving security threats and regulatory mandates.

2. Security Responsibility

Tuya will undertake comprehensive security management and operations for the software SDK, APP, modules, and services, and data interactions on its cloud platform, and will assume the relevant responsibilities for the security of its cloud service platforms and infrastructure.

When clients use Tuya's services, they should independently develop, manage and maintain their Apps or embedded hardware software (which includes SDKs) that connects to Tuya's cloud, and ensure the security and regulatory compliance of their applications and data (as detailed in section 2.2), which includes the security compliance of hardware and Apps.

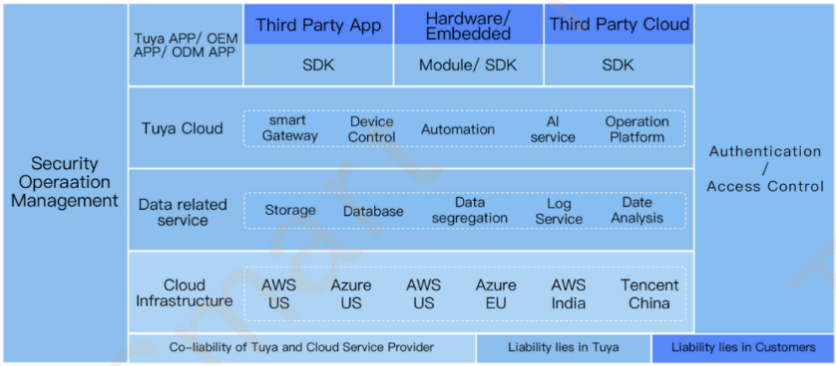
Clients are entirely responsible for the security of the applications they develop and should implement suitable security measures to safeguard their applications and data from unauthorised access, use, disclosure, damage, or interference.

Tuya will provide clients with the necessary technical support and security guidance to help them ensure their application and data security and compliance.

Nevertheless, clients are ultimately responsible for the security and compliance of their applications and data. Tuya does not assume any liability or losses resulting from this.

Clients and Tuya should cooperatively work together to assure the security and compliance of the services that Tuya offers. Should any security or compliance issues be found, both the client and Tuya should immediately inform each other and collaboratively address the issue.

The following image represents the shared responsibility model between the fundamental cloud service provider, Tuya, and the client, with regards to information security responsibilities:



2.1. Tuya's responsibility for security

Tuya Cloud collaborates closely with leading global public cloud service providers such as Amazon, Microsoft Cloud, Tencent Cloud, and Alibaba Cloud to ensure the physical security of data centers and the stable, compliant operation of fundamental cloud infrastructures.

Tuya Cloud provides Platform as a Service (PaaS) level business and data security coverage. Tuya is committed to continuously bolstering the platform's overall security capabilities and defensive systems by leveraging its security team and collaborating with renowned security service providers worldwide. It also offers secure operational and management services for the cloud platform, effectively ensuring the secure operation of business on Tuya Cloud, while safeguarding customers' and users' data security and privacy compliance. The primary coverage includes but is not limited to:

- Data security: Refers to the secure management of business data within a cloud computing environment, including collection and identification, classification and leveling, authority and encryption, and privacy compliance;
- Access Control Management: Management of access rights to resources and data, including user management, permission management, and identity verification;
- Cloud Service Security: Pertains to the security management of business-related application systems within a cloud computing environment, including the design, development, deployment, configuration, and usage of application and service

interfaces.

2.2. The customer's responsibility for security

When customers employ the solutions offered by Tuya Cloud services, they must adhere strictly to Tuya's security configuration and service access requirements. Moreover, customers should ensure the security of their own cloud, client, or intrinsic hardware products to avert potential security threats or vulnerabilities.

For Apps and smart devices developed using Tuya's SDK, Tuya offers essential technical support but cannot guarantee comprehensive security coverage for the entire App and smart hardware itself. Hence, customers are required to take adequate security measures on their own accord to ensure the security and compliance of their Apps and smart devices.

Regarding OEM Apps based on Tuya's solutions or Apps with customized services provided by Tuya, customers need to maintain and update user agreements, privacy policies, and other pertinent policies as per their situation. They should take responsibility for their privacy policy disclosures and legality. When needed, Tuya's security compliance team is willing to lend aid and consultation services for security solutions, to help customers comply with relevant legal and standard requirements.

3. Security and Privacy Compliance

Tuya complies with globally recognized security standards and industry requirements, integrating them into our internal control mechanism, and scrupulously implementing them during the rollout of cloud platforms, Apps, embedded systems, and hardware products.

Tuya holds membership in the China Household Electrical Appliances Association, the Smart Home Appliances Cloud Interconnectivity Working Group, and leads the Smart Home Appliances Cloud Interconnectivity Security Group, having initiated the formation of China's Smart Home Cloud Interconnectivity Information Security Standard.

Tuya has participated in authoring the Smart Home Appliances Information Security Standard set forth by the National Committee for the standardization of Digital Technologies in Intelligent Buildings and Residential Areas.

Furthermore, Tuya is a participant in the China Communications Standardization Association and has contributed to the drafting and establishment of related IoT standards.

Simultaneously, Tuya collaborates with independent third-party security services, consultancies, and auditing bodies to ascertain and ensure the compliance and secureness of Tuya’s cloud platform and the entire value chain.

We perpetually consider information security and data compliance as the bedrocks and protective assurance of our corporate growth, guaranteeing continuous investment for privacy compliance, R&D security, business security, and intrusion defence. We maintain deep-rooted cooperation with top global security firms and privacy compliance consultancies and auditing firms, guiding and fostering the structure of industrial standards. Repeatedly undertaking numerous certifications and compliance audits crossing the realm of information security and privacy security, we pledge to provide data and privacy safekeeping for our customers. This includes the below mentioned compliance ventures:

3.1. Security Compliance Certification & Evaluation

Tuya continually enhances and refines our information security management and technical systems in line with global information security standards. We offer our customers cloud services that have undergone rigorous auditing by independent, third-party evaluation, and certification bodies.

3.1.1. ISO/IEC 27001

ISO/IEC 27001 serves as a globally recognized standard for Information Security Management Systems (ISMS), delivering best practice guidance for the establishment and operation of information security management systems across various organizations. As per the standard stipulations:

- Adopting a business risk-oriented strategy to establish, execute, operate, monitor, review, maintain, and enhance information security;
- To safeguard the confidentiality, integrity, and accessibility of information, setting up a corresponding organizational framework, establishing a systematic security management regime, and guaranteeing resource security;
- Adhering to the PDCA (Plan-Do-Check-Act) model to consistently advance the management of information security.

3.1.2. ISO/IEC 27017

ISO/IEC 27017 sets forth guidelines for information security aspects of cloud computing,

proposing the specific implementation of cloud-focused security controls, thereby complementing guidelines laid out by the ISO/IEC 27002 and ISO/IEC 27001 standards. This code of practice offers advanced guidance on implementing information security controls for cloud service providers.

Tuya Cloud, with several years of dedicated effort and initiative, has actively endorsed the enactment of ISO/IEC 27017, an action that not only showcases our commitment to adopting internationally acknowledged best practices, but also demonstrates that Tuya Cloud's platform is equipped with a high-accuracy control system that specializes in cloud services.

3.1.3. CSA STAR

Ensuring the security of IT networks and data is imperative for businesses. STAR Cloud Security Assessment is a unique and innovative service designed to tackle specific problems related to cloud security, acting as an advanced version of ISO/IEC 27001. To respond to prevailing business issues, the Cloud Security Alliance (CSA, a non-profit organization dedicated to promoting best practices in cloud computing), designed and introduced the Cloud Control Matrix (CCM), which involves frequently employed control measures relating to cloud security, collectively formulated by an industrial workgroup.

Tuya's participation in the STAR Cloud Security Assessment project signifies a significant stride in progressing towards international standards and anticipated advancements within the cloud security management system industry.

3.1.4. ISO 9001

Tuya Smart is ISO 9001 certified. Originating from the first-ever global quality management system standard BS 5750 (authored by BSI), ISO 9001 is, to date, a highly developed quality framework worldwide. It's a comprehensive guideline and regulatory construct used for ensuring the quality of company products and operations, pivoting on the products or services provided by businesses. It revolves around the complete procedure of strategizing, executing, and bettering product or service implementation, endeavoring to meet consumer demands as well as pertinent legal and regulatory requirements.

Implementing a quality management system enables the effective and efficient realization of intended quality objectives. Distinct corrective and preventive measures are adopted following an audit and management review of the quality management system. Persistently enhancing the efficiency of the quality management system stands as the fundamental pillar for the growth and advancement of businesses.

3.1.5. AICPA SOC2 Type II & SOC3 audit report

The SOC2 & SOC3 audit, a prestigious certification in the field of information security and privacy compliance dictated by the American Institute of Certified Public Accountants, serves to guarantee that service providers are managing their data securely, thereby

safeguarding both the interests of companies and the privacy of their clients. Tuya's successful accomplishment of the SOC2 & SOC3 audit authenticates its industry-leading capabilities in preserving customer privacy and ensuring data security.

3.1.6. Level Protection Evaluation Level 3

By passing the Level Protection Evaluation, it signifies that Tuya Smart fulfills the security standards corresponding to the third level of 'GB/T 22239-2008 Information Security Technology - Information System Security Grade Protection Basic Requirements.' It also ensures that the customer's information systems on Tuya Cloud align with the technical and administrative requirements of Grade Protection Level Three compliance.

3.2. Privacy Certification & Verification

Tuya is dedicated to safeguarding the personal data of our global clientele, and adheres to the privacy laws and regulations of the jurisdictions where we conduct our operations.

3.2.1. ISO/IEC 27701

Tuya Cloud has achieved the ISO/IEC 27701 Privacy Information Management certification, further validating Tuya's commitment to international standards of privacy rights and data protection.

ISO/IEC 27701 Privacy Information Management is a privacy extension to the ISO/IEC 27001 Information Security Management System and ISO/IEC 27002 Security Controls. It is an international management system standard system that provides guidance for the protection of personal privacy, including how organizations should manage personal information and assist in proving compliance with privacy regulations around the world.

The emphasis is on control measures for privacy protection, defining management processes, and offering practical guides for safeguarding Personally Identifiable Information (PII) while promoting continuous development. It integrates the most effective practices from ISO27001, ISO27001, and ISO29100. It's the most recently published version among relevant standards, closely aligning with the current issues of privacy protection.

3.2.2. European GDPR Verification Project

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.

Tuya has completed GDPR validation and adopted internal data security protection in accordance with compliance requirements. For more information, please refer to our letter of validation here.

3.2.3. California Consumer Privacy Act (CCPA) Compliance Project

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 officially completed its CCPA compliance audit. The company demonstrates a commitment to compliance efforts and will continue to strive for compliance with the CCPA by dedicating to achievement of its objectives in this regard. For more information, please refer to our letter of validation here.

3.2.4. Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) Compliance Project

PIPEDA refers to the Personal Information Protection and Electronic Documents Act in Canada. This particular act stipulates the manner in which personal information should be dealt with in the sphere of trade and commerce within Canada. It has been designed to shield personal information from unauthorized access, usage, or disclosure and bestow individuals with control over their own information.

Tuya Smart has completed an assessment program of its PIPEDA compliance, demonstrating Tuya's continuous efforts towards global privacy and security compliance. Tuya aims at fulfilling the current privacy laws whilst striving towards enhancing its level of Privacy Protection. Tuya is committed to continuing its efforts to ensure its products and services fulfill the privacy protection needs of customers worldwide.

3.2.5. EPC - TRUSTe Enterprise Privacy Certification

Tuya has officially been awarded the Enterprise Privacy Certification (EPC) and has secured the privacy certification symbol. Being certified by EPC demonstrates that Tuya has fully implemented its privacy policy and privacy controls. EPC enhances Tuya's capabilities in privacy and corporate data management.

3.3. Smart Hardware Solution Security Certification

3.3.1. ETSI EN 303645 certification

ETSI EN 303645 is a technical standard related to the security of consumer electronics IoT products, and it has been released by the European Union. The objective of this technical standard is primarily to prescribe regulations for the security of consumer IoT products and their related provisions. Furthermore, the standard also implicates certain business IoT products under its scope. It is designed to establish a line of defense against potential security threats for consumer IoT products and thereby safeguard user privacy. It provides assistance in ensuring that IoT products conform to security design

principles and supports network security and compliance with GDPR in Europe and for IoT products globally. The Internet of Things Act that is currently being promoted in the UK is also based upon the technical stipulations of this standard.

Tuya Smart's twelve modules such as WBR1, WBR2, WBR3, and TYWE1S have successfully passed the ETSI EN 303645 evaluation and certification by TUV SUD. This achievement signifies that Tuya's WiFi, BLE, and Zigbee smart hardware solutions adhere to the European Union's technical security standards for consumer electronic IoT products and also aligns with the user data protection rules of GDPR. The attainment of this certification demonstrates that Tuya's product offerings - be it Tuya Cloud, Tuya Smart mobile terminal, or Tuya Smart module products - all have received third-party endorsement aligned with GDPR. Going forward, Tuya Smart will persist with its drive to explore and develop progressively more secure products and services.

3.3.2. NISTIR 8259 Security Certification

The NISTIR 8259 series of standards, released by the United States' National Institute of Standards and Technology (NIST), serves as a foundation standard for manufacturers and service providers of smart devices. It is also one of the most comprehensive and widespread effective measures for protecting consumers from network security threats. These standards encompass six core network security capabilities for intelligent devices, including device identification, configuration, logical access to the interface, software and firmware updates, and network security status awareness for smart devices.

Tuya's series modules such as CBU and ZSU have secured the NISTIR 8259A evaluation report, indicating that the security aspect of the smart product solutions offered by Tuya has stepped up yet another notch. The constant enhancement of security measures enables Tuya not only to aid developers in the European and American markets to produce smart devices that comply more closely with local network security industry standards but also provides significant support for Tuya in maintaining its leading position within the IoT network security sphere.

3.3.3. ioXt Product Security Certification

The ioXt certification is a globally recognized and the only industry-driven global security

certification program for the Internet of Things (IoT). The ioXt Alliance is spearheaded by tech and device manufacturing heavyweights including Google, Amazon, T-Mobile, and Comcast. Products and apps that have achieved the ioXt SmartCert instill greater confidence in consumers and retailers within this intensely interconnected world.

As of now, Tuya has secured the ioXt certification for two apps and nine modules. These include Tuya Smart app, Smart Life app, and the module models WBR3N, CB2L, CB2S, CB3L, CB3S, CBLC5, CBLC9, CBU, and CBU-ipex respectively.

3.3.4. PSA Certified Certification

PSA Certified is an independent IoT security framework and certification scheme, established in collaboration with Arm and six industry-leading security companies and evaluation labs with the aim of facilitating large scale deployment of secure IoT solutions. Securing the PSA Certified Level 1 accreditation signifies that Tuya's developed TS24-U module for Matter over Thread has been given an assurance of secure standards from its design phase through to its deployment, boasting appropriate security measures and defense mechanisms to effectively combat security breaches and potential risks. Consequently, developers are able to not only provide their Matter devices with essential information security capabilities but also bolster user confidence in the product's credibility.

Tuya has its dedicated internal privacy compliance team that closely follows industry trends and keeps up with the primary global standards for security and privacy compliance, as well as the laws pertaining to information security and privacy protection in various countries. By teaming up with third-party security service agencies and privacy protection-related law firms, Tuya carries out real-time audits verifying the compliance of its operations. In recent years, taking into consideration the user data protection laws of countries like Canada and India, IoT-related bills in the UK, California, and Washington

State, as well as the standards for information security practices recommended by the EU, Tuya runs thorough internal audits and risk assessments, ensuring all its services and products meet these considerations.

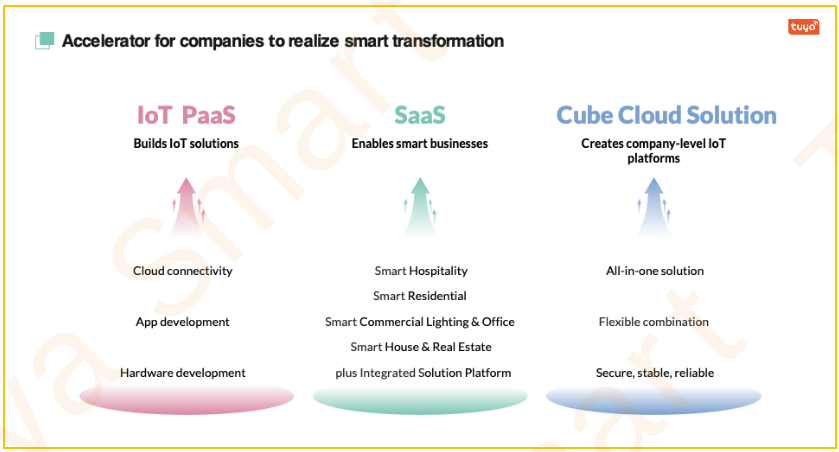
Currently, Tuya is also conducting additional certification audits and, in the future, customers can expect more authoritative third-party audit reports and certifications.

3.4. Compliance Internal Audit

To guarantee the consistent effective implementation of the company's information security management system and privacy compliance system, Tuya has designated compliance control personnel. This team conducts at least one internal audit annually, which involves inspection, supervision, and evaluation of the organization's internal control, compliance management, and risk management. As part of this audit, it verifies if our information security management activities are aligned with standards such as ISO/IEC27001:2013, ISO/IEC27017:2015, ISO/IEC27701:2019, CSA STAR Cloud Security certification, AICPA SOC2 TypeII level 3 protection, and whether they comply with laws and regulations including GDPR, CCPA, PIPEDA. It also checks if we meet the regulations stipulated by the high-standard information security management system in the industry and assesses the effectiveness of the information security management system, following up with corrective actions as per specific areas of non-compliance.

4. Security and Privacy Compliance Architecture

4.1. Tuya Business Architecture



Tuya’s core operations are subdivided into three components:

- IoT PaaS, primarily involving cloud, hardware, and app development. The open model of Tuya IoT PaaS capitalizes on providing a comprehensive IoT solution equipped with a competitive edge that sparks innovation and caters to global clients.
- SaaS is designed to support various vertical sectors in their journey toward intelligent transformation. Tuya proffers an integrated "4+1" solution that includes four standard SaaS services—Tuya Renting, Tuya Hotel, Tuya Business & Buildings, Tuya Household & Community — and a comprehensive solution formed by integrating product capacity components based on aforementioned SaaS services.
- Cube equips businesses across diverse sectors and scenarios to swiftly establish a private IoT platform that promises functional differentiation, system stability, and data autonomy. These three core businesses collectively serve as an "accelerator" driving the intelligent transformation of enterprises.

4.2. Tuya Security Compliance Architecture

Tuya's security and compliance architecture predominantly focuses on four aspects: the

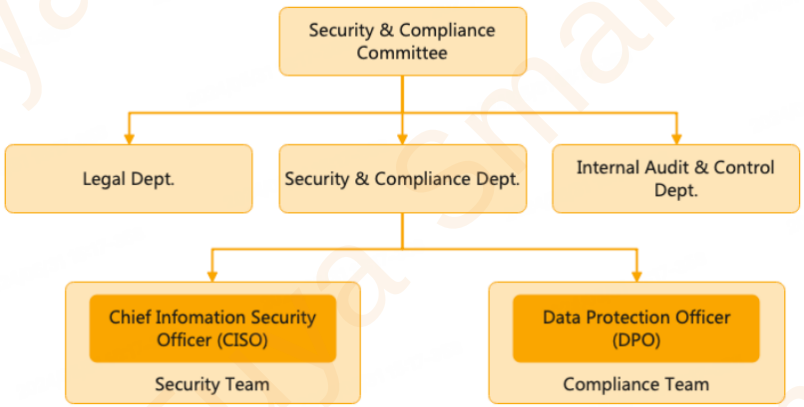
development of a security system, a security protection system, the establishment of a secure hub, and the construction of privacy security compliance. The primary goal of the security system development is to guarantee the security quality of Tuya's products and services. This is achieved by conducting stringent code reviews and tests to assure product security and stability. The security protection system is designed to counteract network threats and ensure the security and stability of operations. Tuya employs a range of security technologies and controls like firewalls, intrusion detection systems, and data encryption to mitigate external threats and prevent data breaches. The security hub is developed to empower businesses at a larger scale, providing technological support for security compliance. By creating a unified security management and service platform, robust security management and support services are offered to various business units thus enhancing the overall security posture.

The Security Center serves to empower businesses at a greater scale, acting as technical back-up for security compliance. By creating a unified security management and service platform, it ensures that various business departments have adequate security management and support, thereby enhancing overall security standards.

Privacy and security compliance is achieved through the harnessing of both internal and external resources. TUYA prioritizes user data protection and privacy, adhering to relevant legal regulations and policy requirements, while employing compliant technology and measures for protecting user data and confidentiality. Concurrently, in collaborative efforts with partners, we are advancing the establishment of privacy and security compliance mechanisms, hence delivering safer, more reliable services to our users.

5. Security and Compliance Organization

To boost the cybersecurity awareness of all Tuya staff and better protect customer interests and the credibility of our products and services, Tuya fosters a philosophy of "security is everyone's responsibility." This leads to the development of a pervasive and ever-present cybersecurity culture rich with vitality and competitiveness. This culture influences every corner of Tuya's operations, from talent acquisition and onboarding to role-specific training, continuous development programs, internal transitions, and even exit procedures. Each Tuya employee actively contributes to the establishment and upkeep of security standards for our products and services, undertaking various security activities as per our regulations.



5.1. Security and Privacy Protection Team and Personnel

Tuya boasts a proficient and comprehensive cybersecurity team, which includes former employees of internet giants like Alibaba, Ant Group, Baidu, and traditional security manufacturers such as NSFOCUS, Qihoo 360, and DBAPPSecurity. Their expertise upholds the security quality, evaluation, and operations management functions of Tuya Cloud. Additionally, the team's competencies extend to privacy and security compliance with professionals from institutions like State Street Bank and externally contracted privacy security agencies. Global and regional law firms with emphases on cybersecurity and privacy protection also provide professional consultancy services. This ensures that

the security and compliance framework within the company is controlled, trusted, and reliable every step of the way.

5.2. Compliance Committee

Meanwhile, Tuya has internally instituted a Compliance Committee, spearheaded by the pivotal founders, inclusive of the CEO, CTO, CFO, and other top-tier management. They jointly pledge their support for information security and privacy compliance. The adoption of uniform objectives for information security, coupled with adherence to legal and compliance requisites, serves as the foundation to provide Tuya, encompassing its operations and vested business entities, with backing in risk mitigation and regulatory compliance. The Compliance Committee convenes formally each quarter to reflect on the cumulative achievement towards security compliance objectives, affirm principal aims for subsequent periods, and foster the propulsion of compliance-centric endeavors.

5.3. Personnel Security Management

Tuya's approach to human resources management aligns with the enterprise's overarching framework, both firmly rooted in legal principles. Concurrently, the "Basic Human Resources Policy" implements standardized procedures across various sectors, from recruitment, contractual employee management, attendance protocols pertaining to information security, to structured separation methods, all aimed at bolstering the management of personnel security.

Prior to extending any job offer, the HR department rigorously scrutinizes the background of prospective candidates to ascertain that their qualifications and personal history fit Tuya's operational needs. It's obligatory for employees to adhere to all laws, company policies, procedures, and the stipulations of Tuya's Code of Conduct. Moreover, each staff member possesses the requisite knowledge, skills, and experience expected of their role.

Upon recruitment, Tuya mandates that employees sign a legally binding employment agreement conforming to the set standards of information management and security regulations. Additionally, they are obligated to sign a confidentiality agreement, which imposes a defined scope of secrecy, safeguarding sensitive and confidential data

inclusive of Tuya, its employees, and clients. This protection extends to trade secrets, technical secrets, employee data, along with the privacy details of customers or users. Access or usage of company resources is only permitted and granted upon successful completion of these agreement signings.

In cases of employee departure, stringent automated and manual approval processes are in place, inclusive of stipulations for job transition and the retrieval of resources and assets such as electronic devices, servers, and various accounts, prior to severance. Senior and specialized roles are subject to additional mandatory compliance audits, scrutinizing workplace behavior preceding departure among other aspects.

5.4. Security Awareness Education and Discipline Constraints

To enhance network security awareness among all employees, mitigate risks related to breaches of network security, and ensure the smooth running of operations, Tuya has issued an 'Employee Information Security Manual'. Regular educational sessions on network security awareness are conducted, rooted in this manual, requiring ongoing learning and understanding of network security among employees. Employees should know what behaviors are permitted, and those that aren’ t, realizing that they must be responsible for their actions even without malicious intent, and pledged to act as per guidelines.

Tuya's 'Employee Information Security Manual' acts as a reference point for employee's security consciousness and behaviors, with comprehensive security awareness assessments and training sessions conducted quarterly, regulating the security procedures for routine office tasks. Teams that meticulously adhere to the information security manual and effectively implement security norms are publicly acknowledged, and formal punitive measures are in place for those violating security protocols and procedures, ensuring that security is taken seriously by all.

Tuya's security team conducts irregular internal drills every quarter, making company-wide announcements about employees with low security awareness levels.

5.5. Security Systems and Technical Training

To ensure that all employees have a clear understanding of the company's information

security management policy and to effectively drive and implement the security strategy, the Tuya Security Team together with the Internal Audit Team conduct quarterly training sessions focused on privacy protection compliance and data protection. Strict pass requirements are enforced for these assessments, with employees failing to meet the requirements expected to continue learning until they successfully pass.

The information security training encompasses both online and offline curriculum which includes, but isn't limited to, secure development training, penetration testing training, vulnerability training, cybersecurity architecture training, regulatory compliance training, secure development process training among others.

6. Data Security and Privacy Protection

Tuya consistently follows the business principle of 'prioritizing user value ', and our top priority is to foster long-term, trustworthy relationships with our customers. To accomplish this, we've designed an encompassing and organized data security framework. This system is developed around the full life cycle of data security, applying a combination of management and technology to ensure every stage - data collection, storage, processing, transmission, sharing, and deletion - is meticulously managed and controlled. We strive to present our clients with robust data security guarantees through this scheme, ensuring the integrity, confidentiality, and accessibility of user data. This further deepens our clients' trust in us and sets a firm foundation for long-standing collaboration between Tuya and its users.

6.1. Principles of Data Security and Privacy Protection

Tuya's products and services always follow the principles of legality, fairness, necessity, and transparency when handling personal data. Listed below are our core principles:

- Principle of Accountability: Tuya is consistently held accountable for its personal data handling activities. We shoulder the responsibility for any harm inflicted upon the legitimate rights and interests of users.

- Principle of Purpose Limitation: We ensure all purposes of personal data processing are legal, fair, necessary, and explicit. The gathered information is solely for these stated purposes and would not be exploited for unrelated objectives.
- Principle of Consent: Prior to personal data processing, we distinctly inform users about the purpose, technique, scope, and rules of data handling, securing their explicit authorization and consent.
- Principle of Data Minimization: Unless otherwise concurred with the user, we process only the minimum personal data necessary to fulfill the purpose of authorized agreement by the user. We refrain from collecting, storing, demanding, providing, or transmitting data irrelevant to the service. Upon achieving the intended purpose, the related data are promptly removed in accordance to the agreement.
- Principle of Transparency: We reveal to our users, in a lucid and comprehensible manner, the range, objectives, and rules of personal data processing, ensuring users thoroughly understand how their data is utilized while accepting oversight from users and third parties.
- Principle of Security: We always uphold a security capability commensurate with the security risks at hand, employing suitable management strategies and cutting-edge technologies to safeguard the confidentiality, integrity, and availability of personal data.
- Principle of Data Subject Participation: We respect and uphold users' rights over their personal data. Users have the liberty to access, rectify, or erase their personal data at any time, and can revoke their previous consent or terminate their account when they wish.
- Principle of Continuous Improvement: Alongside the ongoing advancements in technology and regulations, we perpetually refine and optimize our data security strategies and procedures, ensuring alignment at all times with the best practices and legal requirements.

These principles constitute the bedrock of Tuya's data security and privacy safeguarding. We dedicate ourselves tirelessly to ensure every user's data security and privacy rights

receive the utmost protection.

6.2. Data Ownership Statement

Tuya profoundly comprehends the significance of personal privacy and is unwaveringly devoted to guarding user data. As per data protection laws globally, Tuya's current business model defines the following roles concerning data ownership and handling:

- Data Owner: The individual user owns their personal data.
- Data Controller: In products or services that Tuya offers to corporate clients, Tuya's corporate clients form legally binding contracts. These clients determine the purpose of personal data collection, scope of the collection, and methods of processing - their directive authority effectively makes them the data controllers.
- Data Processor: Tuya dutifully offers continuous service to personal data processing per the instructions of the client, ensuring and enhancing the uninterrupted provision of our agreed services to the individual users.

As a service provider and a data processor, Tuya acts as the trusted entity for customers' data handling, bound by a rigorous data processing agreement, outlining the scope and methods of data handling.

To address the challenges of global data compliance, Tuya has stationed numerous independent data nodes worldwide, deploying a localized data storage and processing strategy. Such an approach aids in complying with different legal requirements across nations and regions while enhancing data security by minimizing cross-border data transmission. Additionally, Tuya enforces rigid data encryption protections ensuring the utmost security of user data throughout its transmission and storage.

Tuya remains committed to staying abreast with the latest developments in global data protection laws, incessantly refining Tuya's data security framework to guarantee the security and conformity of user data.

6.3. Safeguarding Personal Privacy Rights

In today's landscape, data security and privacy protection laws stress the safeguarding of personal privacy rights. Tuya has developed a thorough in-house response process for personal privacy rights, ensuring the utmost realization of user's personal rights while

rendering services.

Simultaneously, Tuya extends help to customers in addressing user privacy requests, which specifically encapsulates the following personal rights:

1) Protect User's Right to Be Informed

- Tuya App and website's privacy policy
  - The privacy terms clearly inform the users of all personal data or types of personal data collected by the application.
  - The privacy terms explicitly convey to users the source and objective of the collection of the stated personal data.
  - The privacy terms clearly advise the users regarding the identity or category of the third parties who can access the aforementioned personal data.
  - The privacy terms periodically notify users through means like emails, App pop-ups, etc., at the same time, important changes in the content like the collection of new types of data, collection of sensitive personal data, and application of data for new utilities, this version of the privacy agreement needs explicit authorization from the users to urgently provide services.
  - The privacy terms clearly afford users with a channel to express complaints, suggestions, and feedback. If users harbor any questions regarding the devices, personal data, or any legal policies, they can channel their feedback through this means.
- Website Cookie Disclaimer
  - It exhibits all Cookies and their respective functions.
  - Functional cookies and advertising cookies enable the user to disable them in a single click, which doesn’ t impact the website's functionality.
- User revokes consent
  - It permits users to rescind their consent while using services like App or WEB. Post withdrawal of consent, Tuya will cease to process the respective personal data.

- In a bid to analyse patterns of utilization of products or services offered by Tuya and provide improved user experiences, Tuya will analyse the data presented and reported by users, and review users' issues while using the products in real-time. Users can disable data analysis in the Tuya APP
- To deliver personalized products and custom-made services, Tuya will process user account information, usage details, and device data. If a user doesn't consent to Tuya's proposed handling, they can disable this option in the privacy settings of the application.

2) Right to Access

Tuya users have the capability to access the personal data collected by Tuya via the App, without the necessity for extra technical assistance.

Tuya users can request Tuya to provide details regarding the processing and utilization of their personal data.

3) Right to be Forgotten (Right to Deletion)

Users, being the data owners, have the ability to deactivate their user accounts and fully erase their data by using the account deactivation feature or by providing feedback/submission via the App, or by reaching out to customer service on the official website. The deletion covers a broad range of data including users' identity information, usage history of the App and smart devices, and any user data produced and accumulated during smart device usage.

When the following stipulations are met, users can request removal of specific personal information:

- Under the following circumstances, the user requests to delete the personal information which should be deleted promptly:
  - Tuya violates laws and regulations, collecting and using personal information;
  - Tuya violates the agreement with users, collecting and using personal information.
- If Tuya violates laws and regulations or breaks the agreement with users to share

and transfer personal information to third parties, and the user requests to delete them, Tuya should immediately stop sharing and transferring behavior and notify third parties to delete them in time;

- If Tuya violates laws and regulations or the agreement with users for disclosing personal information publicly, and the user requests to delete it, Tuya should immediately stop the behavior of public disclosure and publish a notice requiring the relevant recipients to delete the corresponding information.

4) Right to Rectification

If users find that the personal information they have provided is incorrect or needs to be updated promptly, they can manually adjust it within the App. If the App does not offer the capability to alter specific information, users can use the Tuya APP feedback mechanism or use the customer support email to facilitate these changes.

5) Right to Data Portability

Users can request the transfer of their personal data provided to Tuya to another data controller via feedback mechanisms in the Tuya App or through a customer's email contact.

6.4. Data Lifecycle Security Management

At every stage of the data security lifecycle, we have corresponding security compliance management systems, access controls, process management, and security technology measures in place.

6.4.1. Data Collection

Tuya adheres to core data protection principles and respects individual privacy rights when collecting data. User consent is our primary legal basis, and data collection is initiated, ensuring users are informed and abiding by the necessary services principle.

Data collection is authorized only after a thorough risk and compliance evaluation conducted by the compliance team during the need or plan design phase, before formally entering the R&D process. Meanwhile, the compliance team periodically undertakes a Data Protection Impact Assessment (DPIA), analyzes sensitive data for

compliance, and ensures lawful and compliant data collection.

6.4.2. Data Storage

- Data Retention Policy

The retention period for personal information is limited to the shortest time necessary to achieve the intended purpose. Beyond this retention period, upon customer request, Tuya will delete or anonymize user data and securely return the data to the customer. Therefore, Tuya adopts the principle of **minimizing data retention periods**:

- The retention of user personal information is limited to situations where the user has explicitly consented to the use of their personal information for service-related purposes. It must not be used for any additional purposes without user consent. The company internally collects and maintains the time-sensitive information regarding how long these data should be retained.
- Data that is legally required to be retained or data that the company can demonstrate is necessary for business purposes may be retained within the time specified by a clear data retention schedule.
- In accordance with the principle of **minimizing data retention periods**, customers have the right to decide on the data retention policy and promptly inform Tuya for service purposes, etc. When customers request data deletion or data return, Tuya will follow these explicit instructions accordingly.

- Data Storage Region

Six major data centers: China's Tencent cloud and Alibaba cloud dual cloud data centers, Western US AWS data center, Eastern US Google Cloud data center, European AWS data center, Western Europe Azure data center, and Indian AWS data center. The data centers are physically isolated from each other. Tuya provides regional data services according to the user's registered location.

- China: The data is stored in the Shanghai data center in China, with Tencent Cloud providing basic cloud computing support, only providing IoT cloud services for users in mainland China.
- United States: The United States is divided into western and eastern data

centers, the western data center is located in Oregon, with Amazon AWS providing basic cloud computing support, and the eastern data center is located in Northern Virginia, with Google Cloud providing basic cloud computing support. The default services and data of the US region are stored in the West AWS data center as default, and customers can choose whether their services use the East Google Cloud data center.

- EU Region: Europe has two data centers, one in Frankfurt, Germany, with Amazon AWS providing basic cloud computing support, and one in Amsterdam, Western Europe Azure data center. The default services and data of the European region are stored in Frankfurt, Germany, and customers can choose whether their services use Western Europe Azure data centers.
- India: The data is stored in the Mumbai data center, with Amazon AWS providing basic cloud computing support.
- Other Countries: According to the principle of proximity, choose the closest data center in Oregon or Frankfurt for storage, and more regional data centers will gradually be opened up, and multiple regional data centers are currently under construction.

- Data and File Storage Security

In order to cater to specific needs across various business scenarios, Tuya Cloud offers a diverse range of data storage services. We understand the critical nature of data security, and hence, employ the AES256 advanced encryption standard to encrypt and store user data, thereby ensuring its security both while in transit and at rest. For user sensitive data, we implement dual encryption, creating a double layer of protection that significantly enhances data confidentiality.

When managing highly sensitive data, we perform necessary anonymization. This involves keeping the data's effectiveness intact while removing or substituting any part that might disclose user privacy, thus minimizing the risk of data leakage right from its source.

Tuya Cloud has employed an all-encompassing KMS (Key Management System) to ensure holistic security of encryption keys. The KMS system not only manages the full lifecycle of keys, spanning their generation, storage, distribution, updating, and destruction, but also implements a series of security measures to prevent any potential key leaks or unauthorized usage.

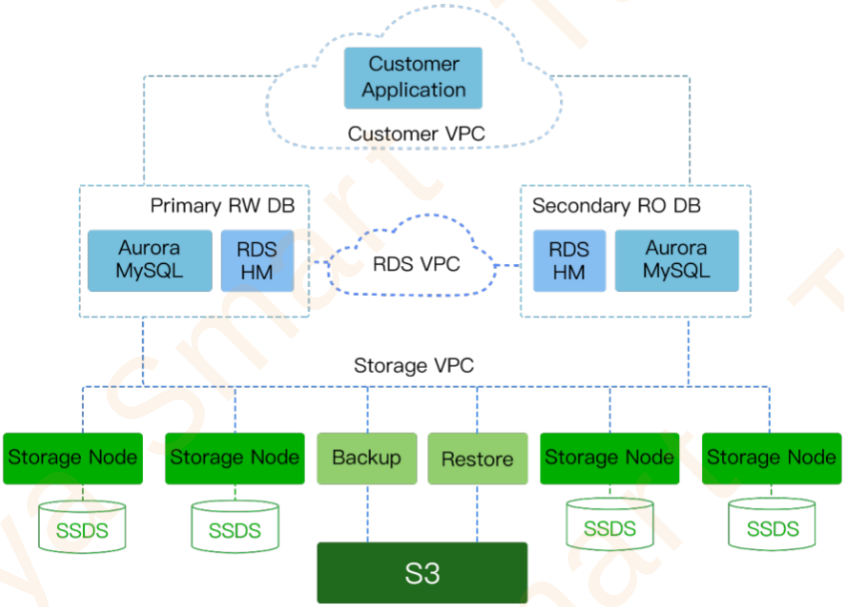
Furthermore, for the protection of sensitive user media information such as images, videos, and other files, Tuya Cloud takes even stricter measures. We generate unique encryption keys for individual users and devices for file protection. This unique one-to-one encryption approach safeguards that even if a file is unlawfully accessed, it cannot be decrypted or viewed without the unique corresponding key, thus maximally ensuring user privacy and data security.

- Redundant Data Storage with Multiple Copies

We use a distributed architecture, wherein all business servers are deployed in three different data centers located within the same city. Database, along with other data storage services, operate under the multi-copy mode, ensuring at least two real-time replicas, and carry out data backup without delay. This architecture provides physical assurance of high reliability and availability of data and services.

All Tuya databases utilize cloud databases, defaulting to the master-slave replication mode with the primary and secondary databases distributed across different availability zones. All disks are local SSD hard drives, supporting auto expansion. Full and incremental data backups are all stored on cloud storage.

We conduct strict data integrity checks during data backup and synchronization across data centers, ensuring the completeness of the synchronized or backup data.



6.4.3. Data transfers

Tuya persistently abides by applicable data protection and privacy legislations, respecting customer preferences and demonstrating meticulous care when collecting, storing and processing customer user data. For our European services, we adhere to GDPR regulations, ensuring that customer user data is securely stored within EU data centers, and we pledge not to transmit this data outside of the European Economic Area. However, under certain specific circumstances (such as providing customer services or technical support), Hangzhou Tuya Company in China might have to remotely access and process this data with customer authorization and user consent. Even though this implies international data transfer, be reassured that all our access protocols are safeguarded by stringent technological and organizational measures to ensure optimal data security.

To ensure that the protection level for personal data aligns with EU fundamental equivalent standards, we have implemented various measures, inclusive but not exhaustive of:

- Tuya has adopted internal data security protection in accordance with compliance

requirements, and has completed independent GDPR privacy practice validation, demonstrating our commitment to and practices in privacy protection.

- Serving as the data exporter, Tuya GmbH, in conjunction with Hangzhou Tuya Information Technology Co., Ltd., the data recipient, has executed valid Standard Contractual Clauses predicated on GDPR stipulations pertaining to the transfer of personal data from the EU to third-party countries, ensuring the legality and security of data transmission.
- Tuya utilizes universally recognized information security standards, such as ISO 27001/27017/27701/CSA STAR, and amalgamates them with industry-leading technology to ensure personal data security and privacy compliance with EU norms.

Beyond strictly adhering to the EU's privacy compliance mandates, Tuya remains vigilant towards the evolving demands of data security and privacy safeguarding in the global landscape. We proactively cater to the legislative compliance necessities for data transmission across different regions/countries/territories, ensuring our operations remain continually synchronized with respective regional legal scripts.

Tuya consistently upholds the tenets of "data localization" and "non-essential, non-synchronization". This implies that user's personal data is predominantly stowed on servers at their locale, preventing unjustified synchronization to other regions. Nevertheless, given Tuya's global operational and management prerequisites, we indeed reserve the right to access and process data across various data centers. These cross-border data processing endeavors are executed under explicit permissions granted as per data protection legislations, conforming entirely to relevant cross-border data transmission regulations.

In conclusion, by harmonizing advanced technology with organizational protocols, adhering strictly to international statutory norms, and maintaining continual vigilance on global data protection flux, Tuya ensures the security, legality, and credibility of data throughout its cross-border transference. We acknowledge the criticality of data and pledge our consistent commitment to addressing the dynamic international demands for data protection and privacy, thereby offering our customers the pinnacle of data security

assurance.

6.4.4. Data Sharing

Tuya collaborates with third-party service providers or business partners, sharing data based on various service requirements and lawful, valid premises, primarily encompassing:

- Providers of third-party intelligent scenario access like Google, AWS, which necessitate users to proactively authorize the sharing of their account data with the corresponding voice platforms, thereby facilitating support for smart home scenarios of Tuya platform users through Google Home, AWS Echo, etc.
- Third-party software service providers to bolster specific services such as SMS and telephony services offered by Nexmo, mobile messaging services by Google or Apple; Tuya adheres to a data-minimization principle when sharing necessary data for these services. If there exists a potential for sharing sensitive data, Tuya imposes a stringent supplier audit on these third-party vendors and collaborators, which includes a privacy and security compliance review.

The sharing of user private data is, in principle, stringently prohibited. If, under certain circumstances, the sharing of private data becomes necessary, a comprehensive privacy risk assessment must be carried out for the said supplier. Simultaneously, users must be informed of the purpose behind the sharing of their private information, the category of data recipient, and prior authorization consent must be secured from the users.

6.4.5. Data Erasure

Any memory or disks that have housed customer data, once released and recovered, will be automatically overwritten with zeroes to clear all information. Concurrently, any storage devices that are to be replaced or removed from use are subjected to a thorough degaussing process and physical destruction undertaken by the cloud server infrastructure provider, prior to their removal from the data center.

6.5. Technical Safeguards for Data Security and Privacy Protection

6.5.1. Data Secure Transfer

- Encrypted Transmission Channels

In Tuya's solution, communication between the application interfaces and the cloud, as well as device and cloud, irrespective of whether it's HTTP or MQTT, utilize the TLS1.2 protocol for data exchange while enforcing rigorous certificate validation.

- Re-encryption of Transmission Content

Communication between the app and the cloud as well as between devices and the

cloud in Tuya's solution is subject to dual encryption using AES128 on top of channel encryption. Special content, such as passwords and biometric data, is desensitized using irreversible hashing algorithms before transmission. Communication between the app and devices, as well as between devices themselves, also employs AES128 encryption for the communication content.

- Data Transfer Integrity

The handling of data transmission within application programs entails integrity checks, inclusive but not confined to communication across devices and cloud platforms, and APP to cloud interactions, typically employing the HMAC-SHA256 algorithm.

6.5.2. Trusted Computing

To ensure absolute data security and trust, Tuya harnesses AWS's trusted cloud infrastructure Enclave, to successfully build the physical trusted computing capabilities of the Oregon data center in the United States. With this state-of-the-art system, Tuya secures comprehensive security signatures for the user data application, code, and their corresponding execution environment, resulting in a reliable environment for the entire data, code, and process management, hence fortifying customer data security.

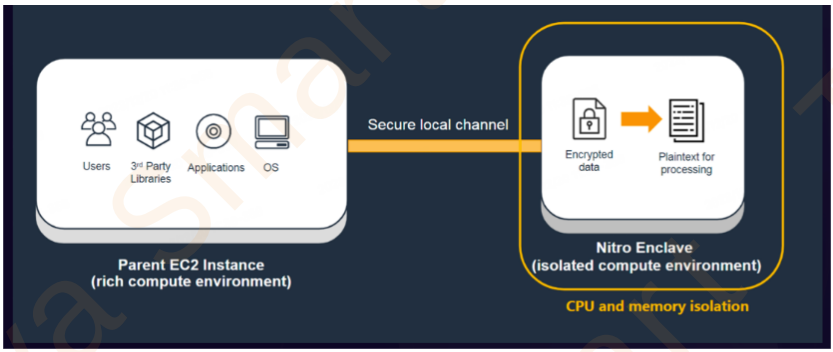
In conjunction, we've integrated AWS KMS (Key Management Service), enabling reliable key hosting and facilitating encryption and decryption operations under a trusted setting. This collaboration tightens key management practices, effectively mitigating risks of key exposure or illicit utilization.

Importantly, within this trusted computation milieu, all alterations regarding user services necessitate re-certification and stringent audits. By doing so, we maintain system stability and security, preventing unauthorized changes from getting approved, thus bolstering user data security and trustworthiness.

A salient aspect of Tuya's trusted computing architecture is that user data, once retrieved from Tuya’s database, can't be decrypted or employed in any computing environment outside the trusted one. This provides absolute data security during transmission and storage, safeguarding against illicit data breaches. Even if data is obtained illegally, without the appropriate key and trusted environment, attackers can't

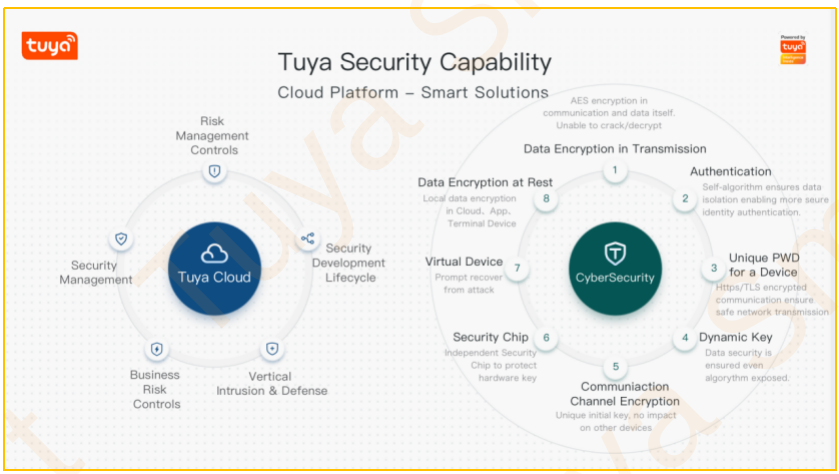
decrypt or use it.

In sum, by merging cutting-edge cloud infrastructure and secure tech advances, Tuya has architected a comprehensive and rigorous trusted computing system, bolstering user data security, confidentiality, and operability at all junctures.



6.5.3. Device End Data Security

Tuya Cloud offers several layers of security strategies to safeguard the data generated by intelligent devices, as illustrated in the following diagram:



- Safeguarding Device-to-Cloud Communication
  - Data Encryption: AES128 is utilized to encrypt data content.
  - Identity Verification: Leveraging Tuya's proprietary algorithm, we ensure secure authentication for device connections, permission requests, and command

dispatch, supporting multiple interaction authentications, access controls, and effective authorizations.

- Dynamic Keys: With a unique dual-code mechanism, we ensure device security.
- Channel Encryption: A full-link TLS1.2 data encryption transmission protocol is employed, with mandatory certificate authentication.
- Security Chip: Select chips provide the option to integrate a secure element for safely storing hardware authorization information and encryption keys.
- Virtual Device Mechanism: Ensures that the compromise of device authorization information does not affect the regular usage of the existing device. Meanwhile, device anonymization technology safeguards user privacy.

- Protecting Device Local Area Network (LAN) Communication
  - Data Encryption: AES128 is used to encrypt data content for in-house/LAN transmission.
  - Dynamic Keys: Dynamic allocation by the algorithm during network setup.

For security measures pertaining to the cloud platform, refer to Chapter 7.

For security measures at the device end, see Chapter 10.

6.6. Data Security Governance

- Data Classification and Grading

Internally, Tuya adheres to strict data classification and grading to clearly specify the extent of data assets, outline principles and assign responsible personnel, as well as establish corresponding data governance requirements.

Based on the source, content, and usage of the data, Tuya classifies the data. The sensitivity level of different data is segregated based on data value, content sensitivity, impact, and distribution range.

As per the 'Tuya Information Classification, Grading, and Processing Strategy,' Tuya Cloud differentiates among personal information, platform information data, and corporate internal data. Depending on the diverse data types and levels, appropriate security requirements and measures are implemented.

- Measures for Data Access Control

- Tuya Cloud employs detailed access control for cloud data and storage. This includes consistent permission control for applications and minimum necessary privilege allocation tailored to different user types.
- Operations carried out on critical or sensitive data are subjected to an internal approval process.
- Separate settings are made for roles of security managers, data operators, and auditors.

- Data Filtering

Tuya Cloud conducts stringent checks on all service entries regarding their data type, length, and format to guarantee data integrity and protection from contamination.

- Data Audit

Full data utilization logs are recorded, including audits of applications or users. For high-risk data handling, the respective compliance auditor's approval is needed for execution.

- Data Display

As a rule, raw data should not be displayed, hence, Tuya adopts de-identification or de-sensitization measures to exhibit personal sensitive data. For distinct business scenarios requiring clear personal data, or to cater to customer data display requests, preventive measures such as mouse hovering or click-to-display are used to inhibit direct user data exposure and diminish the risk of personal information leakage during the display phase.

- De-identification of Personal Information

Following the collection of personal information, Tuya carries out a de-identification process, implementing technical and managerial measures to store de-identified data separately from data capable of restoring personal identity. This ensures that individuals will not be re-identified during subsequent personal information processing.

6.7. Data Leakage Prevention (DLP)

Tuya constructs a synergy of Zero Trust and traditional DLP (Data Loss Prevention) techniques, aimed at curbing data leakage. It achieves comprehensive tracking of data transitions, from download to circulation, to external dispatch in its surveillance model. In terms of data identification, it goes beyond traditional regular expressions and machine learning, incorporating business context-specific identifiers like source applications, file lineage relationships, and so forth. With respect to risk evaluation, Tuya adopts Application DLP, Endpoint DLP, Network DLP, and UEBA technologies to deliver a comprehensive risk assessment in all scenarios.

6.7.1. Implementation of Data Leakage Prevention Technology

1）Supervision of Endpoint Peripheral Transmission Pathways

To mitigate the risk of data leakages, we have imposed a unified external device control mechanism. It allows meticulous management and regulation of external devices used at end points, ensuring that only verified devices can establish a connection with our internal system.

We offer a whitelist control mode, implying that only devices listed in the whitelist are identifiable and usable. This regulatory approach efficiently forbids unapproved external devices from accessing our network, thus considerably curtailing the possibilities of data leaks.

Furthermore, our control function encompasses various external devices and transmission methods, including USB drives, mobile devices, Bluetooth, printers, external network cards, and wireless hotspots among others. We have enforced stringent read/write access controls for each connectivity mode. This implies that even if the device is connected, it cannot perform any data transmission or operations without the relevant read/write permissions, further ensuring data security.

Overall, while ensuring data security, this control method offers enough flexibility and convenience. It allows normal functioning of authenticated devices while effectively

segregating unauthorized ones, ensuring the security of both corporate and personal data.

2) Anti-Screenshotting and Photography via Screen Watermarks

Presently, to further bolster data leakage prevention and regulation, we have initiated a noticeable watermark feature on the computer screens of all employees. The principal purpose of this measure is to deter personnel from arbitrarily taking screenshots or transmitting content containing sensitive information. The presence of the watermark means that any unauthorized distribution activity can be easily traced and identified, hence effectively minimizing the risk of data leakage.

Simultaneously, we acknowledge that under certain special circumstances, watermarks might impose some inconvenience on routine work. Hence, for staff members or departments with special needs, we have implemented an approval mechanism. When required, post stringent approval process, the use of faint watermarks or no watermarks can be facilitated to cater to particular work demands.

This policy attains a balance between ensuring data security and facilitating employee work convenience. It both makes sure that sensitive information isn't leaked easily, and accommodates varying requirements in different work scenarios.

3) Auditing and Interception of Sensitive File Outgoing

In terms of data leakage prevention and control, we have implemented a comprehensive monitoring and auditing mechanism. When employees use instant messaging, email, cloud disk, cloud notes, remote control, code hosting platform and other network channels to transfer files on the computer, our system will automatically carry out sensitive information detection.

Once potential sensitive information transmission is detected, the system will immediately trigger an automated alarm mechanism to notify the relevant managers. At the same time, we have an interception feature that can immediately interrupt the transmission process involving sensitive data to prevent unauthorized leakage.

All file transmission activities conducted through these network channels will be detailedly recorded and audited. The audit logs include the contents of the transmitted

files, time, the network channels used, the employees involved, etc., to ensure that there is complete traceability and review ability for all data transmission behaviors.

These measures integrate automation and human supervision with the aim to minimize the risk of data leakage to the greatest extent and ensure that employees always follow the highest security standards when using various network channels for work.

6.7.2. Data Access Control

Tuya steadfastly upholds the principle of "least privilege" in data processing and profoundly appreciates the significance of customer personal information. To safeguard the security and confidentiality of this information, we've deployed a series of stringent managerial and technical approaches.

For any Tuya personnel authorized to access and process customer personal information, we enforce rigorous permission control. Every employee must undergo explicit authorization and comprehensive training to ensure they comprehend their responsibilities and data processing norms. In order to preempt any form of data misuse or mishandling, we institute precise data management procedures for our staff. Every procedural step must adhere strictly to the company's data security policy.

When Tuya personnel require scrutiny of user data pertaining to customer operations, we install additional safeguards. Employees must not only secure explicit customer authorization but also tender corresponding credentials for approval. Such credentials undergo meticulous reviews by our security compliance ensemble and the legal department. Only after matriculating this stringently scrutinized approval echelon are employees permitted to query anonymized user data.

To ensure every staff member duly comprehends the criticality of data security, we routinely administer data security training aimed at enhancing overall staff security cognizance and operational proficiency. Via such training, we aspire to nurture a company ethos that reveres data and abides by data-handling regulations tenaciously.

Tuya profoundly acknowledges the pivotal role of data security in earning customer trust. We are committed to persistently refining our data security governance infrastructure, ensuring that each procedural step withstands the highest level of scrutiny. Concurrently,

we are open to and appreciate the oversight and assessment by external auditors of our Information Security system, with the aim of continually uplifting our data security benchmarks and methodologies.

6.7.3. Data Security Incident Management

To enhance Tuya's emergency response capabilities for data security incidents, aptly prevent and significantly reduce the harm and effects of data security incidents, and provide assurance for the safe and stable operation of the information systems, Tuya, taking into consideration the "Cybersecurity Law", "Data Security Law", "GDPR","NIS2" and other regulatory policies, and integrating the company's realistic scenario, has instituted and issued "Tuya's Data Security Incident Emergency Management Procedure" and "Data Leakage Prevention (DLP) Event Handling Procedure", among other support systems.

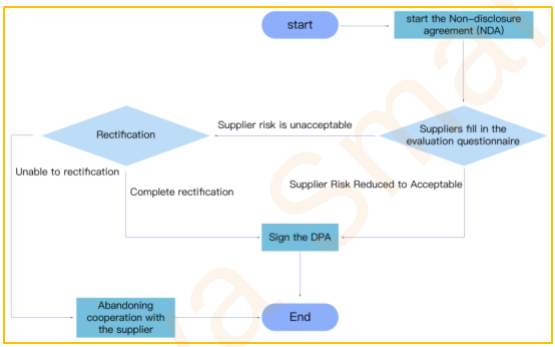
These systems provide a clear standardization for the handling of data security incidents, outlining the responsibilities of involved departments, teams, and individuals, and initiating different emergency response requirements based on the level of incident.

"Tuya's Data Security Incident Emergency Management Procedure" firmly establishes explicit protocols and requirements for everyday security prevention, pre-incident monitoring and alerts, incident handling, and post-incident reviews, providing for an orderly and compliant incident response.

Moreover, the "Data Leakage Prevention (DLP) Event Handling Procedure" prescribes a standard response for incidents occurring during the DLP operation process. This covers the entire incident lifespan from detection, reporting, evaluating, notifying, investigating, handling, reviewing, monitoring, and to continuous improvement, providing explicit regulations. This ensures that in the event of data leakage, swift and effective countermeasures can be executed, thereby significantly mitigating the impact of the data leak on the organization.

6.8. Supplier Security and Privacy Audit

As part of its comprehensive and targeted service offerings, Tuya entrusts reliable third-party data processors to undertake necessary data manipulation activities. Tuya steadfastly conducts audits concerning data security and privacy protection strictly following the "Supplier Audit Process". Depending on the specifics of the product or project, the audit generally involves assessments such as GDPR (General Data Protection Regulation) appraisal, and PIA/DPIA (Privacy Impact Assessment/Data Protection Impact Assessment) assessment. The subsequent steps in the audit process are as follows:



Firstly, leveraging our privacy regulatory assessment toolkit, we administer a security and privacy compliance questionnaire of standard version to conduct a systematic assessment of the suppliers. In case of any intolerable compliance gaps, Tuya mandates immediate rectification, otherwise, suppliers would be barred from our approved vendor list.

The supplier's security capability assessment encompasses multiple aspects including security development lifecycle management process, vulnerability management process, data security lifecycle management process, access control, service and data disaster recovery, personnel and organizational security management, penetration testing standards and support, compliance certification, key management, network security defense framework and facilities, security incident response mechanisms, and change

management among others.

7. Security Assurance of the Cloud Platform

Tuya Smart utilizes the global public cloud infrastructure to enable connectivity and interoperability between smart scenes and smart devices, providing secure, stable, and swift cloud services to clients worldwide. Tuya possesses the capacity to concurrently process massive datasets on the scale of billions, delivering high-stability computing services with an availability of 99.9%. Tuya has integrated the global service nodes of various mainstream public clouds to offer proximate access services for users across all regions, ensuring a smooth and stable device usage experience.

The Tuya cloud platform provides DIY hardware and software development SDKs and a comprehensive and robust set of cloud platform APIs for creators and manufacturers. Offering debugging assistance, we've effectively lowered the development barriers for hardware manufacturers, accelerating the launch of intelligent products. Simultaneously, the cloud platform assists manufacturers in carrying out smart upgrades for their hardware and software, consistently delivering premium intelligent services to consumers.

7.1. Physical Security Measures

As a provider of Internet of Things cloud computing services, Tuya Cloud Platform is committed to delivering secure, stable, consistent, and reliable physical infrastructure to every customer. Abiding by international standards and regulatory requirements specific to data centers, Tuya Cloud has established an all-encompassing security management system, ranging from policy strategies to process management, accompanied by stringent monitoring and auditing. Through ongoing enhancements, the physical and environmental security of the data center on the cloud platform is ensured.

7.1.1. High-Availability Infrastructure

The Tuya Cloud platform synthesizes services from globally revered cloud hosting service providers such as AWS, Azure, Google Cloud, Tencent Cloud, and Alibaba Cloud to construct service nodes worldwide. This formation ensures secure, stable, ongoing, and dependable physical infrastructure for our clients.

Tuya Cloud, leveraging the distribution of submarine optical cables and empirical testing results from cities globally, along with domestic and international sales areas of Chinese companies, configures six available regions covering China, Western Europe, Eastern Europe, the Western United States, the Eastern United States, and India.

This includes but is not limited to AWS data centers in Oregon, Google Cloud data centers in Virginia, AWS data centers in Frankfurt, Azure data centers in Amsterdam, and Tencent Cloud's Shanghai data center. We also run other data centers in various locations including Hong Kong, Singapore, Mumbai, Tokyo, Sao Paulo, and others. The availability zone can be dynamically expanded according to the business client's location.

Tuya Cloud facilitates the flexible deployment of data and systems across different data centers or regions, thereby ensuring the fulfillment of disaster recovery requirements for business operations.

Tuya Cloud provides customers with the ability to specify the location of data storage in circumstances where it is legally permissible.

Server Name	Position	Available Region
Tencent Cloud	Shanghai, China	China Mainland
AWS	Oregon, USA	United States, Puerto Rico, Dominica, Dominica,

		Dominica, Guatemala, Peru, Mexico, Argentina, Brazil, Chile, Colombia, Venezuela, Bolivia, Ecuador, Paraguay, Suriname, Uruguay, Curacao, Malaysia, Indonesia, Philippines, New Zealand, Thailand, Japan, South Korea, Vietnam, Hong Kong, Macao, Taiwan, Myanmar [Burma], São Tomé and Príncipe, Guinea-Bissau, British Indian Ocean Territory, Falkland Islands, French Guiana, Timor-Leste, Norfolk Island, Nauru, Papua New Guinea, Solomon Islands, Vanuatu, Cook Islands, Niue, Kiribati, Tokelau, Palestine, Sint Maarten, Svalbard and Jan Mayen, Åland Islands
	Frankfurt, Germany	Bahamas, Russia, Barbados, Anguilla, Antigua and Barbuda, British Virgin Islands, U.S. Virgin Islands, Cayman Islands, Bermuda, Grenada, Turks and Caicos Islands, Montserrat, Northern Mariana Islands, Guam, American Samoa, Saint Lucia, Dominica, Saint Vincent and the Grenadines, Trinidad and Tobago, Saint Kitts and Nevis, Jamaica, Egypt, Morocco, Algeria, Tunisia, Libya, Gambia, Senegal, Mauritania, Mali, Guinea, Ivory Coast, Burkina Faso, Niger, Togo, Benin, Mauritius, Liberia, Sierra Leone, Ghana, Nigeria, Chad, Central African Republic, Cameroon, Cape Verde, Equatorial Guinea, Gabon, Republic of the Congo, Democratic Republic of the Congo, Angola, Seychelles, Rwanda, Ethiopia, Somalia, Djibouti, Kenya, Tanzania, Uganda, Burundi, Mozambique, Zambia, Madagascar, Zimbabwe, Namibia, Malawi, Lesotho, Botswana, Swaziland, Comoros, South Africa, Eritrea, Aruba, Faroe Islands, Greenland, Greece, Netherlands, Belgium, France, Spain, Gibraltar, Portugal, Luxembourg, Ireland, Iceland, Albania, Malta, Cyprus, Finland, Bulgaria, Hungary, Lithuania, Latvia, Estonia, Moldova, Armenia, Belarus, Andorra, Monaco, San Marino, Vatican, Ukraine, Serbia, Montenegro, Croatia, Slovenia, Macedonia, Italy, Romania, Switzerland, Czech Republic, Slovakia, Liechtenstein, Austria,

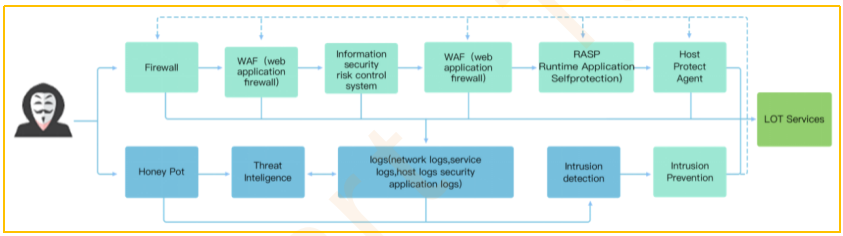
		Jersey, Denmark, Sweden, Norway, Poland, Germany, Belize, El Salvador, Honduras, Nicaragua, Costa Rica, Panama, Saint Pierre and Miquelon, Haiti,, Guyana, Martinique, Australia, Singapore, Brunei, Tonga, Fiji, Palau, Wallis and Futuna, Samoa, New Caledonia, Tuvalu, French Polynesia, Micronesia, Marshall Islands, Cambodia, Laos, Bangladesh, Turkey, Pakistan, Sri Lanka, Maldives, Lebanon, Jordan, Kuwait, Saudi Arabia, Yemen, Oman, United Arab Emirates, Israel, Bahrain, Qatar, Bhutan, Mongolia, Nepal, Tajikistan, Turkmenistan, Azerbaijan, Georgia, Kyrgyzstan, Uzbekistan, Afghanistan, Norway, Comoros, Bosnia and Herzegovina, Saint Martin, Iraq
	Mumbai, India	India
GCP	Virginia, USA	/
Azure	Amsterdam, Netherlands	/

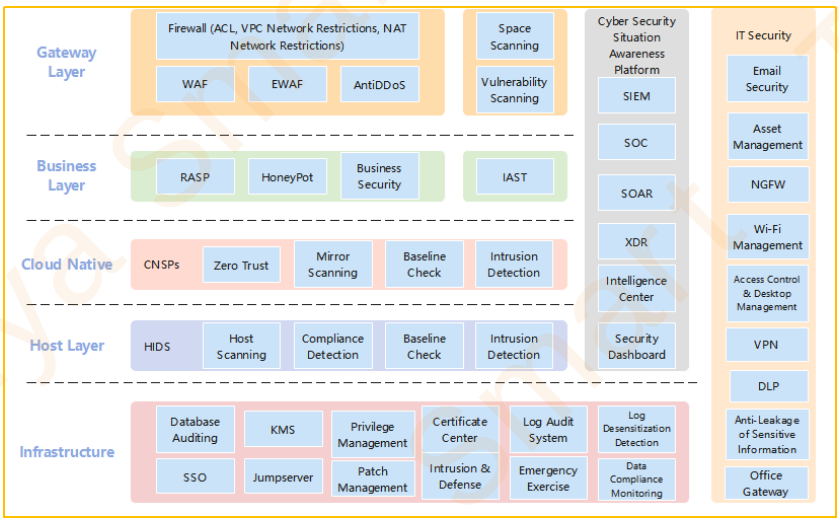
7.2. Network Security

7.2.1. Security Architecture

Tuya Cloud boasts a mature, in-depth network security defense architecture designed to offer full-coverage, fine-grained protection spanning from the network, machine, and application levels down to the code. Our capabilities encompass various protective mechanisms such as Web Application Firewall (WAF), Runtime Application Self-Protection (RASP), Cloud-Native Security Platforms (CNSPs), Host Intrusion Detection Systems (HIDS), HoneyPot, and Security Information and Event Management (SIEM) platforms, in addition to numerous other security applications and components. This approach enables us to identify and counteract various internet threats at multiple layers and dimensions within the technical architecture.

The diagram representing Tuya Cloud's network security architecture is as follows





7.2.2. Network communication security

Tuya Cloud Platform is committed to safeguarding the security of smart hardware solutions, recognizing the critical aspect of communication security. To this end, all communications within our intelligent hardware solutions employ the TLS1.2 security protocol, thereby ensuring rigorous protection of data transmission between devices, apps, and the cloud.

We uphold stringent controls not only over communication protocols but also extend comprehensive security capacities including TLS at the API interface level. This guarantees that irrespective of whether communication with the cloud is via devices, apps, or API interfaces, the Tuya Cloud Platform can offer clients port-level security assurances, safeguarding the integrity and confidentiality of data during transmission.

To enhance security further, we have incorporated AES128 encryption technology to our communication content. This encryption approach uses keys based on random

generation for each device and user, thereby ensuring the keys' uniqueness and security. With this method, we furnish double-layer encryption protection to the communication process, ensuring the security and immutability of data transmission.

At Tuya Cloud Platform, our customers' security always comes first. As such, we persist in adopting the most advanced encryption technologies and measures to provide our clients with the highest level of security protection. We take pride in our professional competence and meticulousness, ensuring you can confidently utilize our smart hardware solutions.

7.2.3. Network Isolation and Access Control

Tuya Cloud Platform acknowledges the paramount importance that network isolation and access control play in ensuring data security. As such, we have put in place several measures to guarantee the security of both internal and external networks.

Internally, Tuya has established rigorous network isolation regulations. We deploy both physical and logical isolation techniques to enforce access control and boundary protection in critical areas such as office, development, testing, and production networks. This approach prevents unauthorized personnel from accessing any internal network resources, thereby significantly mitigating potential security risks.

For staff members who require access to the production network for routine operations, we have instituted a stringent bastion machine approval and permission control system. Employees must achieved suitable permission and undergo a rigorous approval process to use restricted privileges to log into the production ecosystem. Concurrently, we perform thorough auditing of all actions to ensure prompt discovery and management of any irregular activities.

Externally, at the cloud user level, Tuya Cloud Platform proffers a suite of security safeguards. By utilizing a virtualization control layer resource access control strategy, we guarantee that each user can only access resources allocated to them. Additionally, we have enacted separation tactics between the internal private networks of the cloud platform, thereby enhancing data security even further.

Moreover, we authorize permissions and perform identity validation through our WEB

console, assuring that each user can solely access the data and functionalities within their granted permission boundaries. Regarding API interface access, we employ security mechanisms such as session IDs and access keys, thereby guaranteeing the secure transmission and access of data.

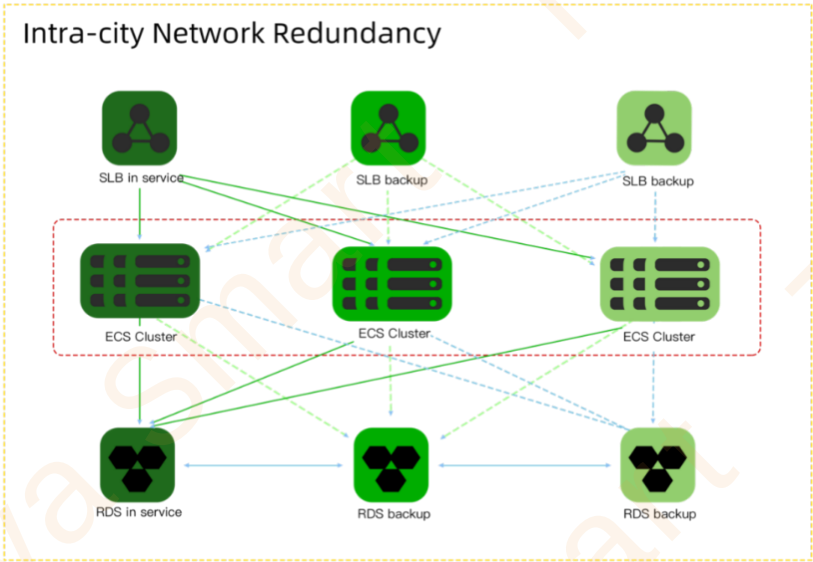
In summary, Tuya Cloud Platform has implemented comprehensive and strict measures in terms of network isolation and access control, committed to deliver the highest level of security protection to our clients. You can rest assured in our professional competence and meticulous approach, and utilize our services with confidence.

7.2.4. Network Redundancy

Tuya Cloud data servers are distributed across numerous global regions, building cross-regional disaster recovery capabilities. This infrastructure can effectively minimize business disruption caused by network malfunctions attributed to non-human factors.

By using a redundant networking structure and implementing multiple physical server deployments within the same city, we achieve networking agility and effective traffic engineering scheduling. This guarantees that network services will not be disrupted due to single-point failures, hence achieving local and cross-city disaster recovery.

The redundancy deployment of multiplexed data center networks within the same city is depicted as per the following figure:



7.2.5. DDoS Protection

Tuya Cloud has constructed our proprietary, high-capacity DDoS protection cluster that is capable of intercepting a variety of DDoS attacks. This includes mitigating IP address scans, malformed packet incursions, and fragmentation onslaughts at the network layer; recognizing and intercepting prevalent transport layer attacks like TCP Flood, UDP Flood, amplification strikes, TCP/UDP fragmented packet invasions, malformed packet charges, and DNS poisoning; identifying and intercepting application layer threats like CC attacks, HTTP slow rate attacks, SSL DDoS invasion, SIP Flood, and MQTT connection assaults. In parallel, Tuya Cloud, to assure business continuity, has activated DDoS mitigation features of prominent cloud platforms such as AWS and Microsoft Azure. This step ensures the protection of all our data centers, granting automatic threat detection, network routing, and threat scrubbing capabilities.

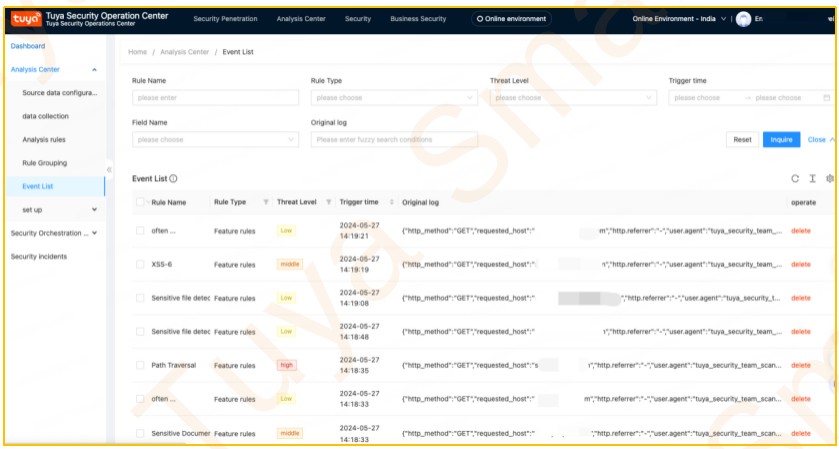
Regarding CC attacks (Challenge Collapsar), we have incorporated firewalls and Web Application Firewalls (WAF) to cap and block abnormal connections. Besides, we analyse all request logs combined with third-party threat intelligence data for detecting abnormal IPs, thus facilitating the dynamic blocking of suspicious source addresses.

7.3. Intrusion Prevention

7.3.1. Network Intrusion Detection

Tuya Cloud Platform remains at the cutting edge of data security. By employing advanced security techniques and strategies, we offer comprehensive protection for our client's business operations. We conduct real-time log inspection and security analytics on all servers, applications, and network traffic, assuring that every data movement is closely monitored. Our current intrusion detection encompasses an extensive range of data that includes the log access of all Tuya's security detection and protective tools, Tuya business gateway logs, DNS service logs, honeypot logs, cloud-native traffic logs, bastion machine logs, risk control logs among others.

The functionalities of Security Information and Event Management (SIEM) system include real-time and post-event analysis of log data to generate security incidents.



We monitor the outbound traffic and DNS requests of our internal business operations through the application of intelligence correlation and anomaly detection technologies. This allows us to promptly identify potential security risks. By combining internal and external network honeypots, honey-bait probes, and services, we are able to swiftly recognize and address threats, thus guaranteeing our clients' business continuity and data security.

In order to enhance our defense capabilities, our platform utilizes both internal

intelligence data and third-party threat intelligence interfaces. Upon detection of anomalies such as IP addresses or domain addresses posing threat intelligence risks, we automatically trigger the blocking mechanisms of our firewall and Web Application Firewall (WAF). This immediate response restrains potential attacks, thereby ensuring data and system security.

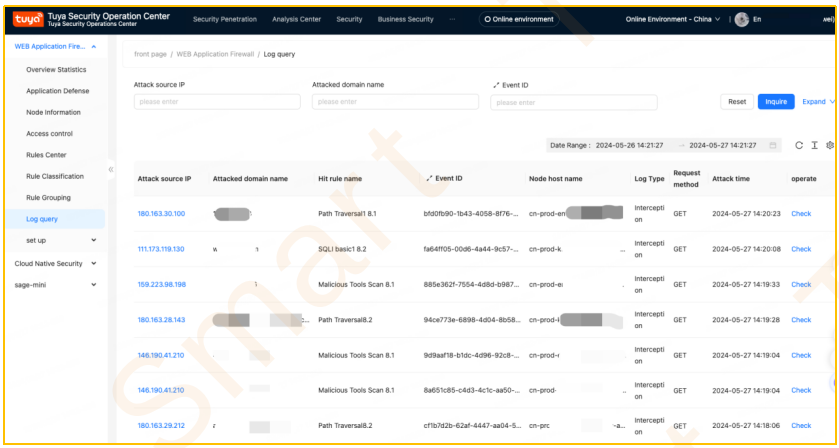
With Tuya Cloud platform, we remain committed to delivering rapid, accurate security risk identification and response capabilities to our customers, facilitated by innovative technologies and strategies.

7.3.2. Network Intrusion Protection

Within its existing defensive framework, Tuya Cloud has activated a suite of security tools that comprise of Web Application Firewall (WAF), Runtime Application Self-Protection systems (RASP), and a cloud-native security platform. These robust protective measures ensure comprehensive interruption and neutralization of potential threats.

1）WEB Application Firewall（WAF）

Tuya's Web Application Firewall (WAF) embodies a design philosophy that unites expert-level protective rules, regular detection engines, and correlated threat intelligence functions. This powerful amalgamation enables it to precisely extract and identify malicious attack requests in real-time within the mass of user request traffic. As soon as malicious activity is detected, the WAF activates its blocking mechanisms. This continuous confrontation and isolation of malicious actors ensure Tuya Cloud's core operations and data security remain uncompromised.



Tuya's Web Application Firewall (WAF) not only facilitates a secure and efficient operating environment for Tuya Cloud's application services but is also armed with a multitude of features to combat diverse network threats. Such features include web application attack defense, CC attack protection, and sophisticated access control functions. Moreover, to guarantee the continuity and stability of services, the WAF employs a high availability architecture. This signifies that it can sustain stable performance and efficient protective capacity, even in the face of large-scale attacks.

Functioning as the outermost defense of Tuya's security protection system, the WAF plays a pivotal role. It quickly recognizes and intercepts external threats, providing the initial sturdy shield for the internal systems, and thereby ensuring the smooth and secure operations of the entire Tuya Cloud platform.

2）Runtime Application Self-Protection (RASP)

Runtime Application Self-Protection (RASP) capabilities can be directly integrated into an application's service, offering function-level real-time protection. It holds the capability to detect and defend against undiscovered vulnerabilities without the need to update policies or the protected application's code.

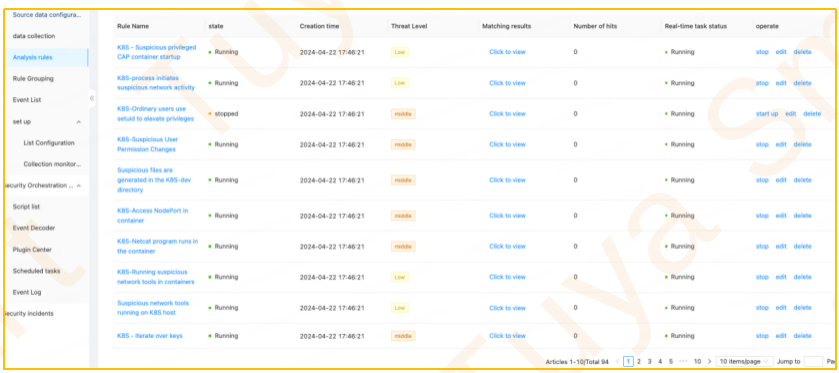
All of Tuya's online business applications have RASP deployed, which hooks on to key functions to monitor the application's execution flow at an in-depth level. At multiple tiers such as the database, network, and file system, it provides thorough auditing and

safeguarding for the application. When an attack is launched, it automatically identifies user input. By collating semantic engines, application stacks, and request instances, it delivers threat detection without adherence to any preset rules.

7.3.3. Cloud-native Security Protection

Tuya Cloud has attained significant strides in the realm of native cloud security. Through the ingenious conjunction of open-source technology and proprietary research and development, we've successfully erected a comprehensive and efficient native cloud security system. This system extends its monitoring prowess deep into the horizontal 7-layer data flow, assuring data integrity and security, while also delivering precise intrusion detection for business layer traffic, effectively countering a range of network attacks.

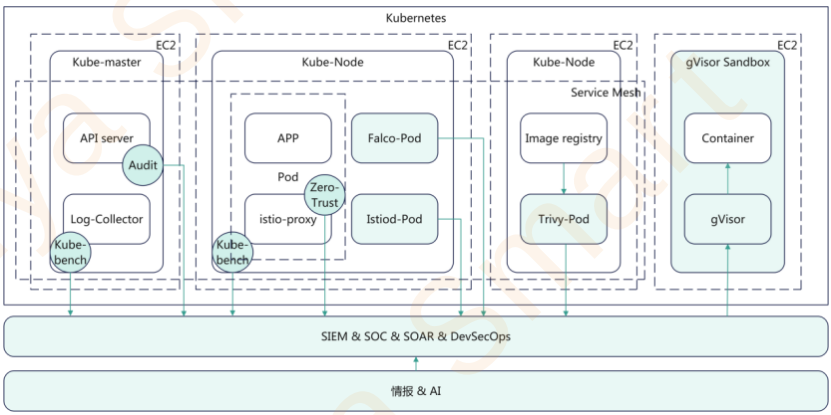
In the context of operational security, we leverage specialized security POD nodes to actualize runtime security EDR (Endpoint Detection and Response) capabilities, signifying our real-time surveillance and analysis of container behavior, all while guaranteeing a safe running environment. Simultaneously, by meticulously sketching and learning communication traffic patterns and combining them with Istio's certificate service, we've constructed a trustworthy chain of links among applications, implemented zero-trust network access mechanisms, thereby further reinforcing our system's security defense.



In the realm of security assurance for the entire cloud-native architecture, we've conducted baseline and image scanning to certify all components and images fulfill high

security standards. Recently, we've incorporated Google's latest open-source cloud-native security sandbox technology. With its concurrent liaison with existing security services, our ability to discern supply chain images and suspicious business activities has substantially improved.

Tuya Cloud continues to lean the helm into the research and development and innovation of cloud-native security technology, constantly refining and amplifying its security protection capabilities. In a world of escalating complexity in the network environment, we remain vigilant to provide secure, stable, and efficient services to our users.



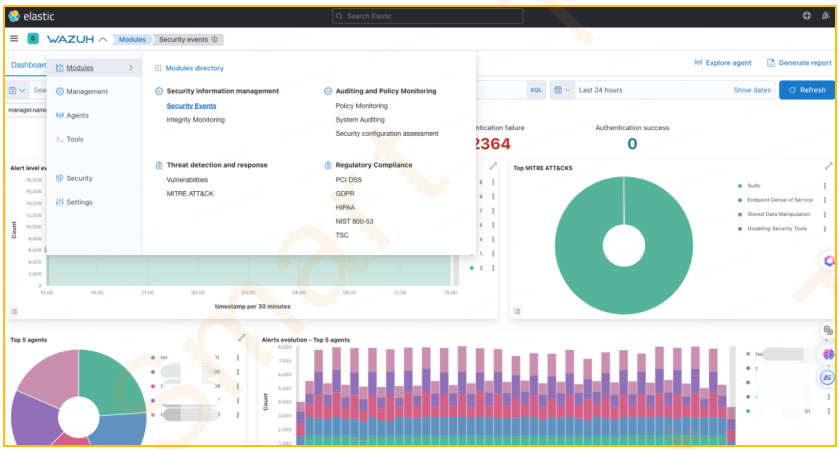
7.3.4. Host Security Detection

Tuya's HIDS (Host-based Intrusion Detection System) network security solution incorporates host monitoring, alerting, log management, and visualization capabilities aimed at threat prevention, detection, and response. Presently, our security proficiencies principally manifest in the following areas:

- Asset Inventory: Wazuh, an integral part of our solution, gather comprehensive information from the monitored system, including details about memory, disk, CPU, interfaces, ports, processes, and applications. This aids administrators in gaining a clear understanding of their system asset standing.
- Security Detection: Operating on the foundation of over 3300 rules, Wazuh is adept at pinpointing hidden files, hidden processes, hidden ports, and malicious file signatures. Additionally, it is capable of executing security audits across Linux,

Windows, Mac, databases, Web containers, and routine infrastructures—like DNS, Active Directory, Mail services, etc.

- Container Monitoring: Wazuh provides in-depth monitoring of containers, encompassing breadth from image examination, detection of configuration alterations, software installation checks, container shell scrutiny, to container vulnerability and process inspections.
- File Integrity Monitoring: Wazuh shoulders the solidarity of supervising the substitution of files residing on cardinal paths, albeit this feature may instigate numerous false positives.
- Vulnerability Detection: Utilizing the local software information paired with the CVE and NVD vulnerability libraries, Wazuh has the capacity to uncover existing system vulnerabilities.
- Compliance Detection: Wazuh facilitates compliance scanning components such as PCI DSS, HIPAA, CIS, assisting businesses in adhering to diverse security compliance norms.
- Active Response: Prompt at detecting security anomalies, Wazuh's endpoint security agents are equipped with the ability to disable accounts, blacklist IPs, amongst other customized actions, actively tackling threats.



7.3.5. Database Auditing

From a security expert standpoint, Tuya's database security audits and role-based access control project a multi-tiered, comprehensive, and exacting security protection mechanism. Here's an in-depth scrutiny of Tuya's database security management:

- Unified Access Management: Tuya employs its Database Management System (DMS) to mandate uniform access rights across its personnel and applications, which is an integral stride towards robust database security. Such consolidation signifies a reduction in the intricacy and potential fallacies in access management, thereby attenuating internal threat hazards.
- Rigorous Access Limitations: A complete audit trail is maintained for all Create, Read, Update, and Delete (CRUD) operations across all databases. In addition, we impose stringent inhibitions on applications' database authorities. Such constraints assure that only approved applications and individuals gain database access, significantly mitigating data leak risks.
- Application Integration and Access Control: Integrating Tuya's database access plugins within the application context and implementing security authentication alongside permission verification- these safeguards assure that an attacker cannot arbitrarily gain database access permissions- even in the event of an application compromise or vulnerability. The plugin's security authentication and permission

checks cast an additional protective veil over database accesses.

- Temporary Key Management: Applications are privy to temporary keys, offering database access matching their respective permissions, exclusively post successful security authentication and permission verification. This temporary key usage strategy enforces stringent authorization for each database access, simultaneously diluting risks of long-term key exposure.
- Encryption/Decryption and Key Management: By coupling with the Key Management Center and KMS services, Tuya bolsters the credibility and security of the application's encryption/decryption procedures. This synergy amplifies data security during transmission/storage and enhances key management's tautness, fending off potential key leaks or misuse.
- Log Auditing and Monitoring: Comprehensive log audits, capturing all CRUD functions across all databases, record potent evidence, instrumental for posterior analyses and assigning blame. Concurrently, it serves as an efficient deterrent, combating unconventional or malicious actions executed by internal personnel.
- Multi-tiered Security Strategy: Spanning from application layers down to data layers, Tuya espouses layered security defense tactics, guaranteeing that security countermeasures from other layers spring into action when a layer falters, thereby offering exception database security.

Tuya's meticulous, strict, and multi-tiered database security audits and access management practices shape an invincible security shield, combating internal and external threats, thus ensuring database security and data confidentiality.

7.3.6. Virus Detection and Elimination

Tuya's dedicated virus scanning service is outfitted with a professional virus screening and eradication software, enabling real-time virus inspection on incremental files and periodically assessing the security of files residing on storage servers. It boasts of a daily-updated built-in virus database, to proactively fend off the latest virus threats. Furthermore, this scanner renders support to an extensive range of archiving formats, for instance, ZIP, RAR, Dmg, Tar, GZIP, BZIP2, along with a plethora of intricate

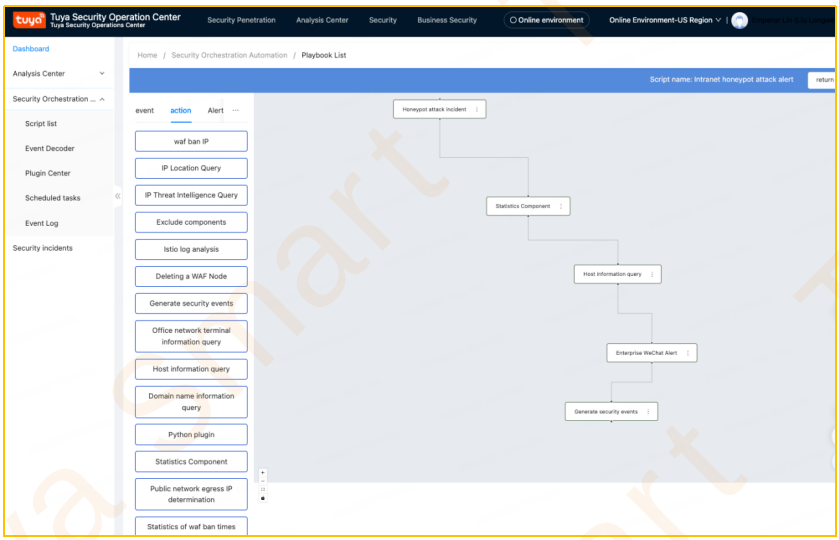
compression and obfuscation techniques, such as UPX, FSG, Petite, NsPack packing techniques, and obfuscation methodologies like SUE, Y0da Cryptor. This substantially barricades any potential hiding or evasive maneuver by viruses.

An important facet of this scanner is its in-built support for an array of popular file formats, including MS Office and MacOffice files, HTML, Flash, RTF, and PDF, facilitating thorough protection against potential virus infiltrations during routine documentation activities. Such holistic backing renders this virus scanning service a formidable ally in system security upkeep, boasting efficiency and comprehensiveness.

7.3.7. Situational Awareness Platform

Tuya's situational awareness platform encompasses the superior techniques of SOAR (Security Orchestration, Automation, and Response) and SIEM (Security Information and Event Management), thereby sculpting a panoramic, multilayered security shield.

SOAR sits at the heart of security operations, effectuating the automated orchestration and intelligent receptivity of security workflows. It uses pre-defined security policies to automatically identify, analyze, and act on a myriad of security incidents, considerably elevating the efficiency of security operations. Likewise, SOAR can be deeply interlaced with security apparatus and systems to effectuate unified management and enactment of security protocols, thereby unraveling the intricacies of extensive security operations.



On the other hand, SIEM serves as the neural center of information security, tasked with the collection and examination of security information and event-specific data from all corners of an organization. Employing big data analysis and machine learning technologies, SIEM can spot potential security threats in real time, offering robust data reinforcement to enterprise security decision-making.

The situational awareness platform, being a fusion of SOAR and SIEM, undeniably equips organizations with an unprecedented ability to safeguard their operations. It paves the way for comprehensive monitoring of an enterprise's network security health and enables the automated response to a host of security incidents, leading to a significant lowering of the organization's security risks.

7.4. Business Security and Risk Control

7.4.1. Account Security

Account security remains a pivotal aspect of the Tuya Cloud service framework. Consequently, we've introduced stringent security management and comprehensive log auditing procedures during critical stages such as account registration, login, password retrieval, and multiple device logins. We've also adopted rigorous protective operations concerning data storage, retrieval, and alterations within the account system.

In specifics, user passwords undergo salted hashing using SHA256 encryption, which proves effective in thwarting password leaks and rainbow table attacks. All the while, our entire account system database employs the AES128 advanced encryption standard, ensuring the security and confidentiality of user information.

To confront common account security threats like database breaches and API misuse, we've implemented precision-crafted policy protections. Currently, all interfaces relevant to sensitive operations, including login and password reset, are equipped with either traceless or sliding captcha technologies. These can accurately differentiate between human users and machine behaviors to effectively stave off malicious activities like rogue registrations and database breaches.

During user registration, we've incorporated a weak password checking mechanism, strictly forbidding the use of commonly weak passwords to decrease account hijacking risks. To accommodate varying customer requirements regarding account security, we also offer flexible security password policy configuration alternatives. Customers can activate Tuya Cloud platform's two-factor authentication as needed, and opt for customized adjustments of various security settings, including APP password complexity, to attain personalized security safeguards.

7.4.2. Content Security

Tuya Company has implemented a unified mechanism of business file type identification at all the file upload points, equipped with state-of-the-art virus scanning and trojan detection engines. This step significantly assures the security and legality of the uploaded files, facilitating swift detection and termination of potential security threats.

Concerning content adherence, we've deployed an exceptional content compliance auditing engine, capable of deeply recognizing a myriad of content types such as text, images, and files. It can effectively pinpoint and filter out potentially offensive, unsafe, or inappropriate content, drastically mitigating the chances of content irregularities and successfully blocking harmful data.

Particularly, this engine is capable of filtering out content that pertains to explicit material, violence, politics, and other illegal or non-adherent subjects efficiently. In the context of

explicit content, it can identify and halt obscene and inappropriate information. While concerning violence, it can detect and prohibit harmful depictions including weaponry, terrorism, and graphic violence. As for politics, the engine is capable of differentiating sensitive from non-sensitive political figures, thus maintaining the political impartiality of the content. Moreover, for foreign markets, it can detect content promoting hate, self-harm, in addition to explicit material and violent content.

With these preventative measures, Tuya's content security service ensures the secure compliance of uploaded files while providing its users with clean and safe digital surroundings.

7.4.3. Key Management

Tuya employs an innovative key management solution, leading to the construction of an unshakeable key management infrastructure. This framework has been designed for detailed governance of the key throughout its lifecycle, encompassing key creation, activation, deactivation, conversion, allocation, backup, and destruction. The solution pays extensive attention to data encryption based on keys, assuring the data's secrecy and integrity.

On the smart device terminals, initial key information is securely inscribed into the device's dedicated security zone during the production stage. After successful completion of device authentication and user binding, the system generates a random key, thus escalating security. The key used for local data encryption is dynamically generated based on the device's information and solely remains valid locally, averting any risk of key exposure.

In terms of the APP interface, we utilize Android and iOS system's keychain service to securely store and safeguard essential keys, ensuring key security across variable application settings.

In a cloud-based scenario, Tuya has set up a unified key management system, seamlessly integrated with leading cloud service providers' KMS (Key Management Service). Any application must bypass strict authentication and gain permission to access and utilize the key system and its related services. This system not only supports

creation, management, encryption, and decryption operations but also incorporates an extensive in-built audit functionality to meet evolving regulatory and compliance demands. With these provisions in place, we guarantee the confidentiality, integrality, and availability of the key, providing customers with an unparalleled level of security assurance.

7.4.4. Certificate Management

Tuya has conducted comprehensive research and development and introduced an efficient and secure certificate management system for server and terminal device certification issues. This system fully capitalizes on the excellent features of cloud computing technology, with its basic structure founded on cloud manufacturer's security certification services, like AWS's CloudHSM facilities, ensuring robust availability and scalability.

Using this system, we can effortlessly perform a series of key operations like certificate issuance, downloading, deactivation, re-issuance, disposal, and importing, effectively covering the complete lifecycle management of the certificate. Importantly, the system comes equipped with client-side modules matching the certificate. These modules enable no-contact certificate installation during code deployment. Consequently, they can automatically execute certification configuration and invocation without manual interference, significantly escalating the convenience and security.

Regarding data storage, the certification management system effectively utilizes KMS (Key Management Service) provided by cloud service providers to encrypt all sensitive data encompassing the certificates. This encrypted storage mode assures that even if data is unlawfully intercepted during transmission or storage, attackers cannot whatsoever decrypt data and access the contents, thus noticeably enhancing system data security.

Additionally, to cater to the diverse needs of different businesses, this system offers certificate issuance and verification function based on numerous dimensions like domain names, terminal information, and firmware details. These functionalities not only starkly diminish the complexity of certificate management but also renders the system flexible

enough to cater to varying practical application scenarios, providing businesses with comprehensive and efficient certificate management solutions.

7.4.5. Configuration Management

Tuya has pointedly included strict configuration management specifications within its extensive endeavors for internal system security. To guarantee data security and system integrity, we sternly prohibit using hard coding for storing crucial configurations in any application, including but not limited to sensitive data like keys, certificates, and database configurations.

Tuya employs a progressive configuration management platform, mandating that all applications must be authenticated before they're allowed access and can solely retrieve the requisite configuration details via the configuration center. This measure efficiently impedes any risk associated with configuration data leakage, hence ensuring data security and confidentiality.

Significantly, our configuration center has been meticulously integrated with the certification management and key management system, thus facilitating a cohesive, efficient configuration management infrastructure. Meaning, operations like configuration modifications, certificate renewal, and key rotations can all be managed centrally on one single platform, drastically enhancing the overall management efficiency and security.

Additionally, concerning application authentication and permission management, we've put forward a stringent approval process. Every business must go through a particular approval protocol prior to invoking configuration, assuring that only authorized applications are given access to corresponding configuration information. This measure effectively halts any unauthorized access and potential security threats.

Tuya's configuration management platform amply exhibits its professional rigor in information security, providing robust assurance for the safe and steady functioning of corporate internal systems.

8. Terminal Security

8.1. APP Client

Tuya has introduced the Smart Life App and the Tuya App, often collectively known as the public version apps, aimed at providing users with convenient and proficient services. These public versions are not only available for free for users to download and use but also boast of several benefits like immediate control, rich scene settings, powerful feature integration, and global utility. Tuya, being the prime developer and operator of these applications, is perpetually committed to delivering a superior user experience.

One crucial point to note here is that this section gives a security overview for public version apps. However, concerning OEM or ODM apps, or third-party applications designed using Tuya IoT APP SDK, the operational accountability lies with the particular APP publishing entity, namely the client themselves. In such situations, Tuya still holds the responsibility for the security of the software information it provides, and pledges to grant necessary information security update services and software technical support.

To assure the overall security of the app, clients need to abide by the best security compliance practices during the development or distribution process, shielding their app to the best possible extent from prospective security threats, thus ensuring user data security and stable application operation.

8.1.1. Client Program Protection

The safeguarding of the client program forms the initial line of defense for the APP client security. We've implemented the following measures to ensure the client program's protection:

- Anti-tampering: We ensure the APP remains unaltered during transmission and operation through performing signature verification and integrity validation.
- Code obfuscation: We escalate the challenge involved in reverse analysis by applying obfuscation to the APP code, subsequently defending the core algorithms and business logic from straightforward cracking.
- Emulator detection and blocking: We identify and thwart the APP operation

occurring within an emulator environment, preventing attackers from deploying the emulator for malevolent activities.

- Root environment detection and alert: We check if the APP operating environment is in a Root environment. If so, an alert is triggered along with the execution of appropriate security measures.
- Debugging prevention: Through technical strategies, we hinder attackers from executing dynamic debugging on the APP, thereby promoting a secure APP operating environment and data security.
- Screen hijacking protection: We avert the extraction of users' sensitive information or execution of malicious operations by blocking screen hijacking attempts.
- Hook plugin detection and process injection defense: We spot and counteract malicious Hook plugins and process injection activities, ensuring the consistent functioning of the APP.

Simultaneously, considering the security enhancement feature for the OEM APP, clients can manually initiate or tailor it within the Tuya IoT dashboard.

8.1.2. Comunication Security

To guarantee the security of communication between the APP and the cloud, we've implemented the following practices:

- Usage of secure protocols: The communication channel between the APP and the cloud employs secure protocols like HTTPS and MQTT over TLS for communication. The certificate information is strictly validated to mitigate the risk of hijacking.
- Encrypted data transmission: The data shared between the APP and the cloud are all protected with AES128 encryption. Furthermore, the encryption Key is a randomly generated dynamic key, established based on each user session, solely valid during the ongoing session, thereby fully securing the data involved in the communication.
- SSL Pinning: We offer support to enable the SSL Pinning function within the Tuya IoT platform for amplified communication security.

8.1.3. Component Security

Considering the four primary components (Activity, Broadcast Receiver, Service, Content

Provider), we've adopted the following security actions:

- We strictly regulate the usage permissions and access permissions of components to avert malicious invocations and data leaks.
- For components developed externally, we execute thorough permission and input verification to ensure the security and legitimacy of the input.
- In regard to the WebView component, we maintain an upgraded version of the SDK, strictly controlling the URL domain name and file access permissions to thwart cross-site scripting attacks and file access vulnerabilities.

8.1.4. Data Security

To safeguard the data locally stored on the client, we've undertaken the following measures:

- Internal storage security: For the necessary local configuration files and other kinds of information, we store them using secure encryption methods and adopt stringent read-write-execution permission settings; we don't store any user-related sensitive data in the SQLite database, and we prohibit the inclusion of sensitive information in Android's SharedPreferences configuration file.
- System log security: The official client refrains from printing and retaining any interactive logcat or log files to prevent potential leaks of sensitive details.
- Keychain data security: We avoid hard-coding significant Keys, utilizing secure algorithms developed in-house for saving keys, thus ensuring key security.
- Memory data security: During significant operations, we do not store user data in memory or promptly erase sensitive data from memory to prevent malicious data acquisition.

8.1.5. Privacy Compliance

Our client strictly complies with international laws, regulations, and prevalent norms for information security and privacy protection. We have laid out a comprehensive protection strategy for users' personal information comprising but not limited to implementing transparency in our collection and usage rules, enhancing the process to strictly adhere to the principle of necessity, explicitly declaring the purpose, methods,

and scope of personal information collection and utilization, refining the user consent solution, and implementing a thorough complaint reporting or manual processing system for user feedback to protect user privacy rights. Detailed information can be found in Chapter 5.

8.2. Hardware and Firmware Security

8.2.1. Device Certification

During the manufacturing process, each Tuya module records a unique set of device authentication information. This data is singular across all devices and is associated with the module's environmental aspects, including elements like the chip ID and MAC address. This information is added when signing the data packet during every session request. To facilitate effective communication, it's imperative that each dialog authenticates the module's environmental data and device authentication information accurately.

8.2.2. Communication Security

Based on various hardware chips' performance, Tuya offers distinct levels of encryption mechanisms to augment the chips' security capabilities, ensuring communication security regardless of the selected encryption mode. At present, the primary communication protocol for Tuya's Wi-Fi modules relies on MQTT over TLS and HTTPS, each utilizing TLS1.2 and AES for double-layered encryption protection. Simultaneously, during the interactive process, an added layer of AES encryption is used to secure data and control instructions. TLS initiates bidirectional identity verification and mandatory certificate validation, while the AES encryption key is dynamically generated based on each device, generating a unique random key. Tuya's Bluetooth protocol, constructed on Bluetooth's secure communication, employs end-to-end encryption techniques; each session generates an encryption key through negotiation, ensuring data protection with an AES128 encryption algorithm. Tuya's P2P protocol ensures total DTLS communication, employing similar end-to-end encryption technology for authentication and data encryption key generation; each session is encrypted, using a uniquely generated data encryption key. Additionally, all of Tuya's communication data

implements a plethora of data protection mechanisms, comprising anti-replay verification, device identity validation, access control, and permission verification.

8.2.3. Firmware Protection

Tuya applies several layers of security to protect the firmware:

- Firmware Read/Write Protection: Depending on the level of support offered by the chip platform, constraints are imposed on firmware read/write access, thereby preventing the firmware from being accessed or altered through hardware means.
- Firmware Encryption Protection: Tuya utilizes built-in firmware encryption provisions made available by certain platforms. In conjunction, Tuya applies its own proprietary firmware encryption mechanism to safeguard core coding.
- Code Obfuscation: Additional protection is applied via code obfuscation to the firmware's core coding sections.

8.2.4. OTA Security

Tuya offers two methods for firmware upgrades: a full firmware update and incremental updates. Various security safeguards are adopted during the firmware upgrade process:

- During the firmware package creation, the packaging tool generates a firmware integrity check sum, composed of several variables.
- When a client requests firmware, the server dispatches the firmware download specifics and the firmware verification data. The firmware verification information uses a safe HMAC signature algorithm, as well as signing the unique ID key information of the device. This ensures the legitimate status of the firmware during transmission and prevents unauthorized manipulation.
- Upon receipt of the firmware, the client calculates the firmware verification data and contrasts it with the server-provided information. Simultaneously, during decompression, the client verifies the integrity check data embedded in the firmware by the packaging tool. The firmware is permitted to be written only after this dual verification process is successfully completed.
- Should the writing process fail or if the firmware malfunctions after updating, it will automatically revert to the original firmware.

8.2.5. Data Protection

Tuya's network modules provide security chips as a key feature, designed to harbor a networking module's authorization information and encryption keys. This authorization data ensures the security and legitimacy of communications between Tuya modules and the cloud, offering functional defense against illicit access or manipulation of authorization data and encryption keys by unauthorized individuals. The security chip is structured to include a secure data compartment. Throughout its operation, the Tuya module transfers the encrypted sensitive data into RAM, which is lost if the power is cut. Moreover, any communication between the module and security chip is protected by temporary key encryption.

In versions not featuring a security chip, essential data security is maintained by encrypting significant locally stored information using AES, post-encryption this data is stored. The encryption key is randomly generated during each chip's initialization and securely saved. This key is solely utilized for local encryption, never applied in business processing or any interaction.

8.2.6. System Security

Tuya's smart hardware solution strictly adheres to minimizing the exposure of local services. During the network setup phase, it opens the necessary port services temporarily, based on actual requirements, thereby ensuring secure communication between the application and the smart hardware. Throughout the communication process, Tuya employs AES128 encryption technology, which effectively upholds the security of data transmission.

Moreover, to support localized communication through a single WIFI protocol, Tuya opens the corresponding communication port locally and likewise applies rigorous end-to-end encrypted communication safeguards, utilizing AES128 for data encryption to ensure the communication process is secure.

In its system design, Tuya persists with a minimalist approach, completely removing redundant system components and codes, such as telnet and ssh, in turn reducing both the system's complexity and potential security risks.

In the aspect of firmware compilation, Tuya exercises secure compilation measures, protecting memory security effectively and mitigating potential attacks and their exploitation.

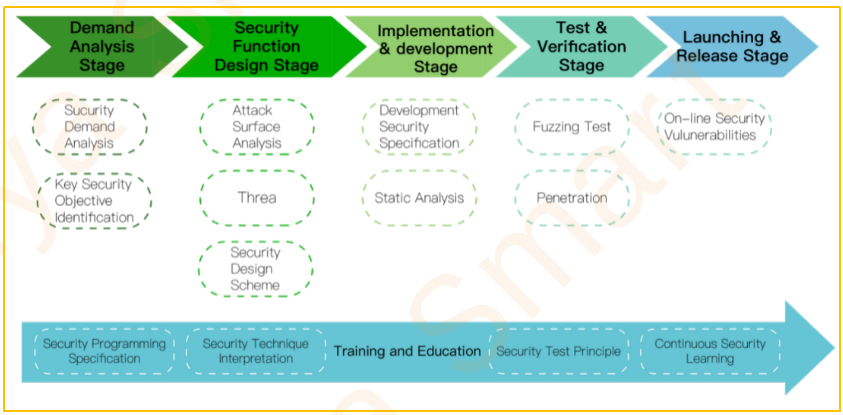
Specifically for unique device classifications, Tuya offers operational service ports, employing stringent system account protections and following a 'one machine, one key' management approach, which assures device security and reliability. These implemented checks compound into Tuya's comprehensive security protection system for its intelligent hardware solution, offering all-inclusive security assurance to users.

Customers or developers creating firmware or systems using Tuya's SDK must independently ensure the security of the entire firmware or system; Tuya only takes responsibility for the SDK.

9. Secure Development Lifecycle Management (SDLC)

Tuya strictly adheres to the Secure Development Lifecycle methodology in the development of services and products for the cloud, apps, and smart devices. Its objective is to incorporate information security into the entire software development lifecycle.

Tuya's secure development lifecycle comprehensively encompasses every phase of the system development lifecycle.

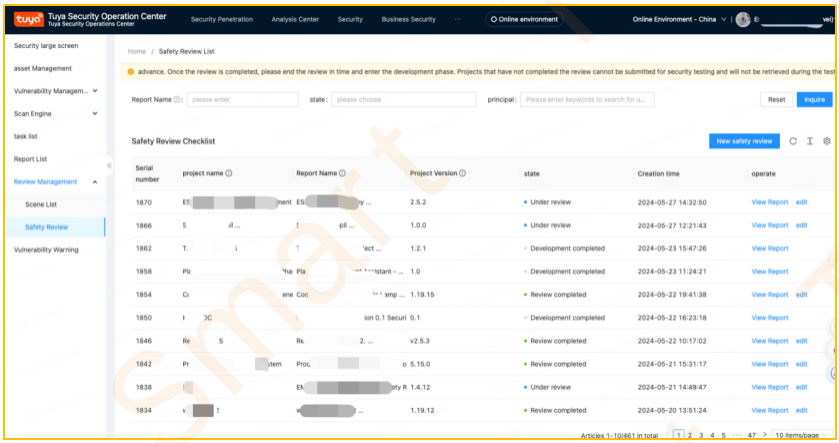


Through a unified Security Management Platform, Tuya effectively oversees and manages the project's SDLC implementation. This approach essentially facilitates fully automated process tracking and automated security assessment.

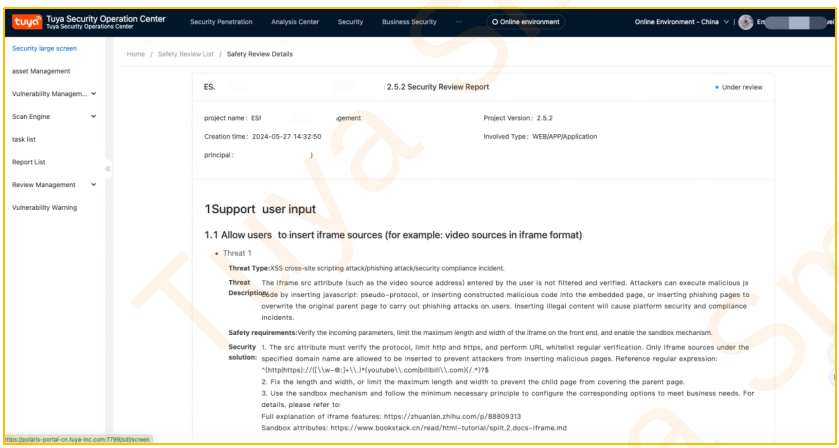
9.1. Security Requirements Analysis and Product Design

9.1.1. Security Requirements Analysis Phase

- Submission of Security Review Requirements: The business team is required to formally submit a security review request on the security platform. They should clearly indicate the specific business segment to be reviewed and attach an exhaustive document detailing the product's security requirements.



- Generation of Security Requirements Report: Based on the context modules previously managed by Tuya's security team and known security risks, the platform will automatically generate an initial security requirements report for the submitted business segment.



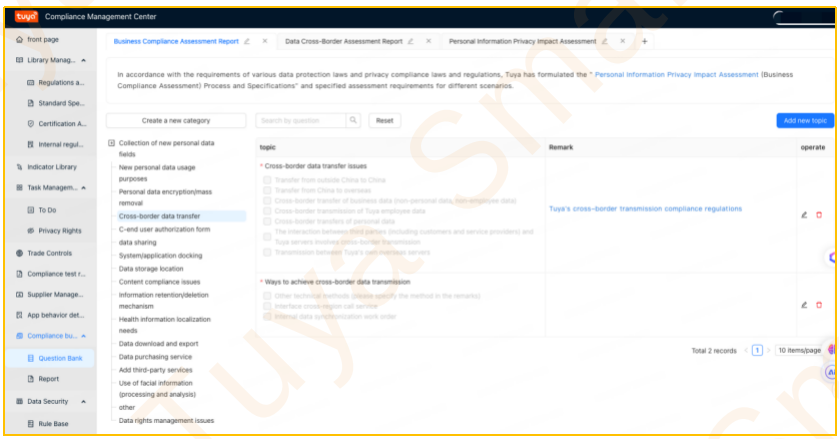
- Annotation and Communication on Security Requirements: If there are scenarios not covered or parts that are difficult to implement in the initial version of the security requirements, the business team is required to clearly mark them during the review process. Upon receiving the annotations, Tuya's security team will actively engage with the business team for deeper discussion concerning specific business logic,

processes, and technical frameworks, ensuring both parties have a clear and uniform understanding of the security requirements.

- Updating the Review Knowledge Base: Based on results from discussions with the business team, Tuya's security team will continuously update and refine the review knowledge database. This ensures that security requirements for similar scenarios in the future can be rapidly and accurately identified and addressed.

9.1.2. Compliance Requirements Review Phase

- Submission of Compliance Requirements: In addition to conducting security reviews, if the business team handles sensitive modules that involve user data analysis, they need to complete a compliance review request. This is done by providing detailed information about the product's possible compliance risks through a questionnaire provided by the compliance team.



- Compliance Risk Assessment and Approval: The company's compliance and legal experts will meticulously evaluate the submitted questionnaire content, carry out a professional review of potential compliance risk items, and ensure that the product design aligns with the laws, regulations, and industry standards.

9.1.3. Product Design Phase

- System Security Analysis: During the initial phase of product design, Tuya's security team will carry out a comprehensive analysis on the system's attack surface – including threat modeling and privacy risk assessment – in order to fully detect

potential security threats and attack pathways.

- Technical Security Evaluation: The team will conduct a strict security assessment on all technologies utilized in the product design to ensure they maintain the capability to withstand typical attacks and effectively safeguard user data and system resources.
- Privacy Compliance Assessment: An in-depth privacy compliance review will be conducted for all data processed by the product, particularly those involving user privacy, ensuring data collection, storage, and usage align with the relevant laws, regulations, and privacy policy.
- Risk Communication and Mitigation: In case of any identified security and privacy risks, Tuya’ s security team will closely work with the developers, providing specific security advice and implementation guidelines to ensure all recognized risks are appropriately dealt with during the product design stage.

9.2. Development Phase

9.2.1. Security Development Guidelines

During the development and coding stages, Tuya's security team implements a series of standard technologies and procedures within the security process management of information security research and development, ensuring the security of the code. Here is a detailed description:

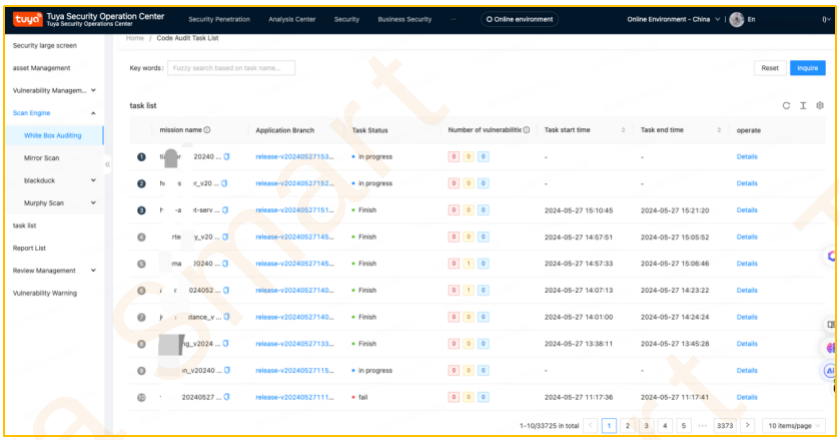
- Security Coding Component SDK: In accordance with industry best practices and international standards, Tuya's security team has developed a collection of secure development components. These components have undergone stringent security testing and adhere to the principle of least privilege, thus minimizing potential security risks.
- Security Coding Guidelines: The team has devised detailed security coding guidelines, which require developers to follow specific programming habits and standards so as to lessen the potential vulnerabilities within the code. These guidelines entail requirements in aspects such as input validation, error handling, and encrypted storage.

- Training and Education: To ensure that developers have a thorough understanding and adherence to the secure coding guidelines, Tuya's security team has provided comprehensive training and educational courses. These courses encompass the fundamental concepts of secure coding, best practices, and how to implement this knowledge in particular projects.
- Automated Verification Tools and Test Cases: Tuya's security team provides the R&D team with automated verification tools and test cases to ensure maximum identification and remediation of potential security risks before the code is committed. These tools can automatically scan the code to detect commonly found security vulnerabilities and provide remediation recommendations.
- Automated Code Audits and Open-Source Component Audits: Anytime the development team accomplishes a code commit, an automatic code audit and an audit of the open-source components are conducted. While the code audit is aimed at identifying potential security vulnerabilities and non-compliant coding practices, the open-source component audit ensures that all open-source components utilized in the project are secure, and there are no known vulnerabilities.
- Prompt Security Patch Notifications: If any risks or vulnerabilities are detected by the automated audit tools, the system immediately notifies the concerned developers. This measure ensures timely and effective remediation of security issues, thereby lowering the potential for security risks.
- Adherence to International Mainstream Coding Standards: The secure coding rules at Tuya are based on not just the company's internal best practices, but also comply with globally accepted coding standards, including pertinent standards from the National Institute of Standards and Technology (NIST), the European Telecommunications Standards Institute (ETSI), and the Open Web Application Security Project (OWASP) guidelines. By adhering to these authoritative standards, Tuya ensures that the security of its codes meets the industry's best standards.

Through the combined application of these measures, Tuya's security team manages to significantly reduce security risks during the coding and development stage, assuring the

security of the company's products.

9.2.2. Code Audit



Tuya's Code Audit Platform is a productive, automated code auditing tool that is seamlessly integrated with Tuya's project deployment system. As the project reaches the pre-release phase, the platform automatically triggers a code audit test to assure the code's security. Below is a detailed description of the standard information security code audit techniques and solutions that the platform employs:

- Syntax Tree Analysis: Leveraging advanced syntax tree analysis technology, Tuya's Code Audit Platform conducts thorough analysis of a project's source code. By creating a syntax tree structure for the code, it can precisely identify critical elements within the code, including functions, variables, control flows, and more, providing a comprehensive security assessment.
- High-Risk Function Identification: This platform has robust function identification capabilities, enabling it to accurately locate high-risk function entries in the code. These high-risk functions may encompass insecure input handling, inappropriate system calls, potential memory leaks, among others. Identifying these functions allows the audit platform to promptly pinpoint potential security issues.
- Forward and Backward Analysis of Function Use: Apart from identifying high-risk functions, Tuya's Code Audit Platform also conducts a forward and backward analysis of function usage. This means it tracks a function's call path in the code and

analyzes function parameter usage. This form of analysis aids the audit platform in detecting potential vulnerabilities that could result from insecure function utilization.

- Multi-Language Support: Tuya's Code Audit Platform supports several programming languages, such as JAVA, C/C++, Python, NodeJS, and more. With this multi-language support, the platform is versatile and can be applied across various projects at Tuya, regardless of the programming language used. This ensures efficient code audits and vulnerability detection.
- Automated Audit Process: The platform is seamlessly integrated with Tuya's project release system, enabling an automated code audit procedure. When a project enters the pre-release phase, the audit platform automatically initiates a code audit test, alleviating the need for manual intervention. This automation not only enhances audit efficiency but also ensures each project has undergone a rigorous security review before being released.
- Vulnerability Database and Intelligence Gathering: Tuya's Code Audit Platform comes with a robust vulnerability database and intelligence gathering capabilities. It collects and analyzes publicly disclosed vulnerabilities, security research findings, and more, continually updating its audit rules and algorithms. This feature allows the platform to quickly identify and address emerging security threats and methods of exploiting vulnerabilities.

With these advanced technologies and solutions, Tuya's Code Audit Platform can effectively assist business teams in identifying potential vulnerabilities within the code, thereby increasing the security of their products.

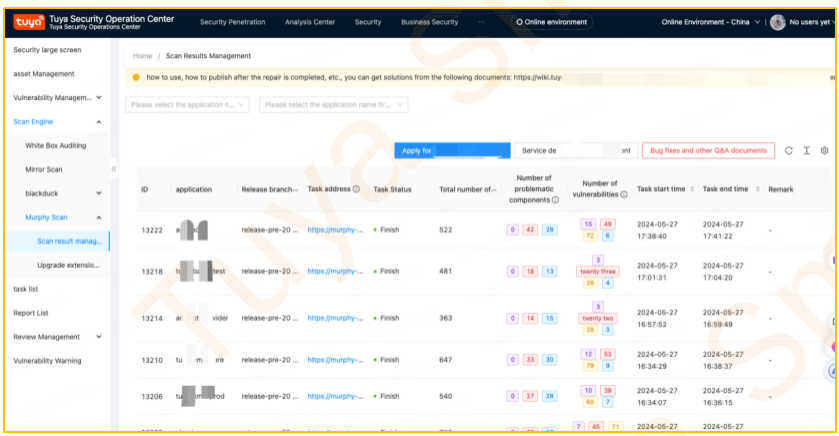
9.2.3. Open Source Audit

Acknowledgeably, the Tuya security team recognizes the importance of supply chain security. Accordingly, it has employed a series of internationally acclaimed solutions and techniques for open-source audits to safeguard information security. Here is a detailed description of the routine techniques and solutions Tuya employs for supply chain security audits, particularly software composition analysis (SCA):

- Deployment and Integration of Murphy SCA: The Tuya security team has selected

the industry-leading Murphy SCA as its open-source audit solution, integrating it intricately with numerous CICD processes. This move guarantees that, before any code is released, all incorporated third-party SDKs or binary firmware bundles undergo stringent security inspections.

- Open Source Component Identification and Tracking: By leveraging Murphy SCA, Tuya can accurately identify and track all open-source components used within applications and containers. This includes directly introduced ones, as well as indirect and nested dependencies. This holistic visibility enables the team to promptly discover and manage potential security threats.
- Open Source Vulnerability Discovery and Remediation: In addition to identifying open-source components, Murphy SCA tool can automatically detect known vulnerabilities within them. Upon detecting vulnerabilities, the system promptly notifies the development team and provides remedial suggestions or patches. This process ensures Tuya can swiftly respond to and amend potential security issues.



- Open Source License Validation and Compliance: Compliance forms a vital part of supply chain security. Murphy SCA tool is capable of validating the licenses of all open-source components used within applications and ensures Tuya's usage aligns with the said licenses' terms and conditions. This mitigates potential legal risks and reputational damage arising from license infringements.
- Standards for Source Code Utilization and Management: Tuya adheres to stringent

guidelines for the use and management of source code. Prior to the introduction of new open-source components, the team conducts a comprehensive assessment of its features, popularity, community development activity, documentation thoroughness, and licensing through Murphy SCA. This rigorous matrix evaluation method certifies that Tuya selects only high-quality and trustworthy open-source components.

- Usage Approval, Testing, and Security Audit: Beyond the comprehensive assessment, Tuya insists on necessary usage approvals, testing, and security audits for all introduced open-source components. This procedure ensures every component adheres to Tuya's security standards and quality benchmarks.
- License Compliance Risk Assessment: Tuya has stringent risk definitions for license compliance and explicitly forbids the incorporation of any components that might trigger compliance risks. This zero-tolerance policy ensures Tuya's compliance and security in the usage of open-source components.
- Advocacy of Security Audit IDE Plugins: In a bid to amplify developer security awareness and coding quality, Tuya also strongly advocates for the use of IDE plugins with security audit capabilities. These plugins can identify potential security risks in real time during the coding process and provide remediation suggestions, thereby mitigating the probability of security vulnerabilities at an early stage.

By implementing these techniques and strategies, Tuya is able to uphold the highest industry standards for supply chain security, effectively safeguarding the security and stability of its offerings.

9.2.4. WEB Vulnerability Scan

Tuya's vulnerability scanner is an advanced security instrument that marries proprietary technology with commercial scanning capabilities, offering a comprehensive and in-depth vulnerability scanning and risk management solution for businesses. Below are its key characteristics and functionalities:

- Integrated scanning capabilities: Tuya's vulnerability scanner brings together its state-of-the-art scanning technology and the merits of commercial scanners,

thereby ensuring rapid security scanning for newly launched businesses, alongside regular profound inspections for all services and applications.

- Constant update mechanism: To tackle the ever-evolving cyber threats, Tuya's security team closely monitors the latest vulnerabilities on the Internet, and timely updates POC, ensuring the scanner is always prepared to identify and guard against the most recent security threats.
- Proactive and passive asset discovery and management: Besides scanning based on the existing asset repository, the platform can also identify network assets both proactively and passively, and autonomously manages them. By leveraging a machine learning model, it can amplify and correlate asset information, facilitating comprehensive lifecycle management of all assets.
- Extensive coverage of vulnerability plugins: The platform integrates thousands of the most recent vulnerability scanning plugins that can automatically recognize modifications in business assets and thoroughly detect vulnerabilities spanning applications, services, and operations. Every plugin undergoes stringent testing and analysis to guarantee zero false positives during vulnerability inspections.
- Asset-centric risk monitoring: As an asset-centric scanner, Tuya vulnerability scanner provides comprehensive surveillance of all exposed asset information and its related corporate sensitive data. By correlating with threat intelligence, it can swiftly identify and respond to security risks triggered by core asset leaks, source code leaks, employee information disclosures, new vulnerability eruptions, and illegal activities.

High-precision detection results: Each detection plugin endures hundreds of automated tests and false positives/false negatives analysis prior to deployment, with the aim to ensure every detection result provided to users is flawless and accurate.

9.2.5. API Security Scan

Tuya's unified API lifecycle management platform is an exhaustive, precise management system aiming to provide efficient, comprehensive management and security measures throughout the entire lifespan of APIs.

Initially, the platform enforces a strict API launch approval registration process. All new APIs or modifications to existing ones have to pass through a specific authorization procedure prior to being launched. This guarantees API quality and compliance while fending off unauthorized or untested APIs from infiltrating the production environment.

Ahead of the API deployment, the platform establishes a significant checkpoint: automated security case testing. This is enabled through the platform's checkpoint interface, ensuring each API undergoes a thorough security audit before going live. These test cases mirror a range of attack scenarios to validate API security and steadiness. Only APIs that pass these tests can proceed with the ensuing release process.

In particular, for interfaces concerning the permission model, the platform adopts stricter management measures. These interfaces must undergo a dedicated security audit prior to release. This scan will delve into analyzing critical security attributes such as the interface's permission settings and access controls, ensuring the interface does not pose any permission-related security risks post-release.

Beyond the aforementioned security measures, Tuya's unified API lifecycle management platform also offers a plethora of management features, such as API version control, traffic monitoring, error log analysis, and so forth. These functionalities aid developers and administrators in better comprehending and managing the operational status of APIs, thereby allowing them to swiftly respond and address any potential issues or risks.

Overall, Tuya's unified API lifecycle management platform, through its rigorous launch approval, automated security testing, and dedicated permission model interface scans, guarantees the security, stability, and compliance of APIs throughout their entire lifecycle. This renders a secure and trustworthy API usage environment for Tuya's developers and users.

9.2.6. Mobile and Firmware Scanning

Tuya's mobile application and smart hardware firmware packaging platform represent a highly integrated, automated solution uniquely designed for Tuya's ecosystem. The platform has successfully incorporated the CICD process for mobile applications as well

as the CICD process for smart hardware solutions, hence accomplishing comprehensive automation from development through to deployment.

Upon completion of the APP or firmware packaging, the platform will automatically channel them to the applicable scan platform for a security inspection. For mobile applications, the scanning platform fully accommodates both Android and iOS systems to ensure that regardless of the operating system employed by the user's device, the Tuya APP can offer the utmost level of security.

Regarding smart hardware, the firmware scanning platform is compatible with multiple prominent chip platforms, guaranteeing that Tuya's smart hardware undergoes thorough and all-encompassing security audits at the firmware level. This cross-platform compatibility allows Tuya to offer unified, efficient security measures for its extensive spectrum of hardware product lines.

By deeply integrating the CICD process, Tuya's mobile application and smart hardware firmware packaging platform has actualized the best practices of Continuous Integration and Continuous Delivery (CI/CD). This not only accelerates the pace of the development and deployment processes but most crucially, through automated security scans, it ensures that every released version adheres to the strictest security standards.

Moreover, the platform also offers an abundance of customization options and flexible scalability to adapt to evolving business requirements and technological environments. Whether it's the incorporation of new mobile application features or firmware updates for smart devices, the platform can rapidly adapt and deliver the requisite security support.

Tuya's mobile application and smart hardware firmware packaging platform, through its high degree of automation, cross-platform compatibility, and continuous security scanning, provides robust security assurance for the entirety of Tuya's product ecosystem. This in turn guarantees that the security of user data and devices consistently receives the most efficient protection.

9.2.7. Interactive Application Security Testing (IAST)

Tuya's IAST solution leverages a hybrid framework that fuses request-oriented and code-centric data flow technologies. This harmonizes the benefits of Static Application

Security Testing (SAST) and Dynamic Application Security Testing (DAST), enabling an exceptionally high detection rate with minimal false positives. It also allows pin-pointing to API interfaces and code segments, and seamlessly syncs with functional testing. This facilitates the highly accurate identification of inherent application security risks, detection of third-party components and their associated vulnerabilities, while concurrently enabling real-time alert responses. This allows for precise location of security vulnerabilities, providing substantial security assurance for deploying the system. Presently, the probing agent of this product has been fully integrated into business applications that passively seek out security risks in the application services.

9.2.8. Deployment Environment Security Scanning

When dealing with the application's deployment environment, which includes aspects such as ports, domain names, servers, and corresponding images, Tuya conducts baseline security audits and employs tools to maintain continuous baseline security monitoring. This includes inspecting for insecure configurations, version vulnerabilities, and conformity to baselines among others. These elements are concurrently integrated into the project process during publication. This measure guarantees not just the quality of the code itself, but also assures the security of the deployment environment.

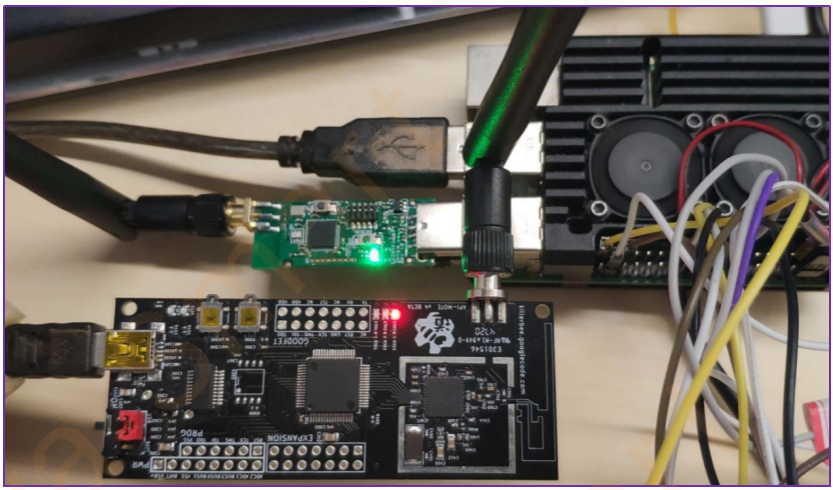
9.2.9. Hardware Security Evaluation Tool

Tuya's security team has strictly established a security compliance benchmark for intelligent hardware products internally. Using test tools, this corresponding security baseline is scanned, after which, a report is automatically crafted and pushed to the hardware distribution platform.

Tuya's smart hardware security compliance benchmark employs mainstream industry information security standards and certification requirements. This includes, but is not limited to, ETSI EN 303645, NIST IR 8259, ioxt product certification, and PSA Certified Level 1 information security standards and certifications.

This security auditing tool, based on the Raspberry Pi as its operating platform, constructs a SoftAP with comprehensive functionality. It also incorporates various security auditing tools, allowing for a quick, low-cost deployment to developers and

testers. This reduces the complexity associated with firmware security testing.

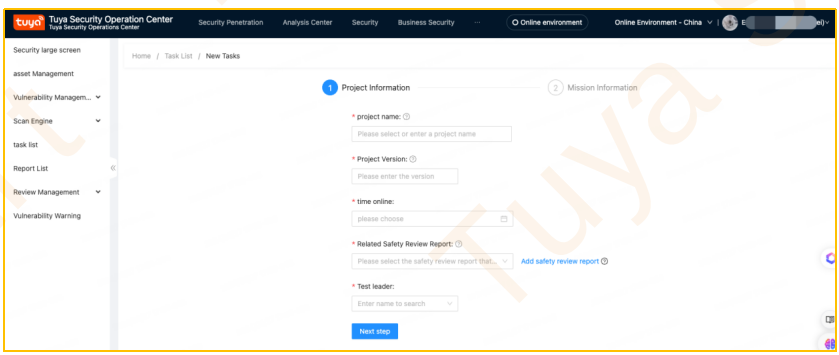


9.3. Security Testing and Remediation Verification

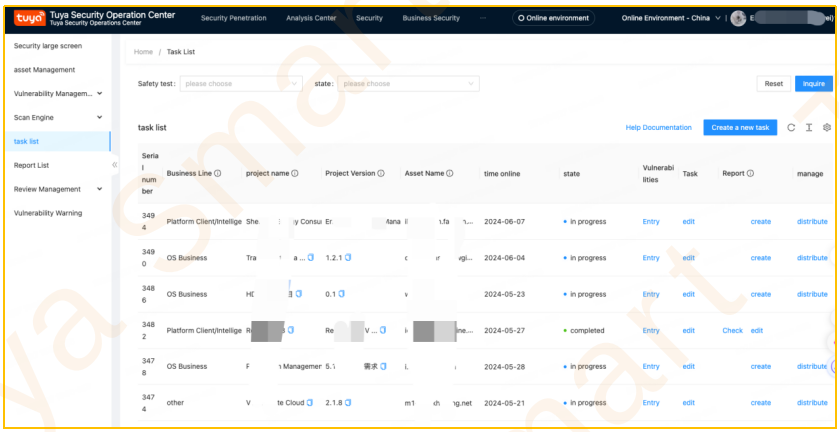
9.3.1. Security Testing

Tuya's project security testing adheres to mainstream industry standards. These include references such as OWASP Top 10, OWASP Mobile Top 10, EN 303 645, OWASP Top 10 Privacy Risks Project, among others.

Upon completion of the security assessments and product development process, the project is required to be submitted for testing on the security platform. The platform then autonomously delegates the tasks to security testing staff. Simultaneously, a clear prerequisite for submission for testing is that it has already passed the security and compliance requirement review.

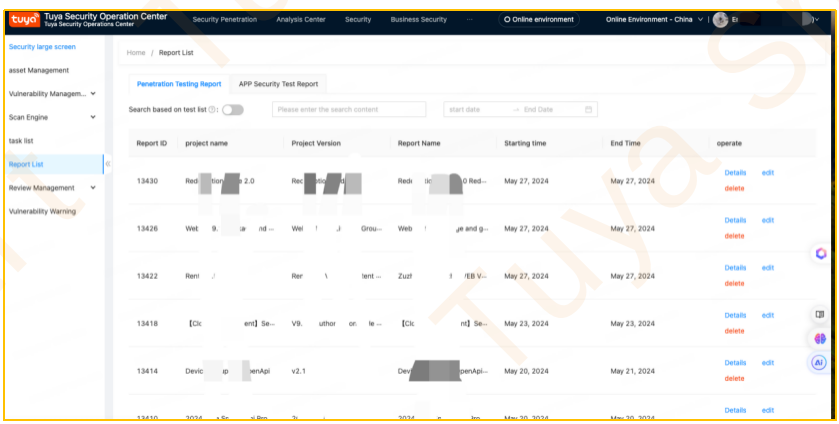


During this testing phase, the Tuya security team utilizes vulnerability scanning platforms, code auditing, mobile scanning and other tools in conjunction with manual testing to carry out security penetration and discover vulnerabilities. Once vulnerabilities are identified, they are tracked for targeted remediation through a work order system.



9.3.2. Vulnerability Remediation and Security Evaluation Report

During the release phase, the system can only be deployed to the production environment if it has undergone security testing, remediated all medium and high-risk vulnerabilities, and obtained a 'Security Testing Report'. This ensures the effective prevention of security vulnerabilities within a product running in the production environment. The release process follows secure deployment standards to bolster the overall system security.



10. Security Operations and Management

Tuya's security operations are managed through a dedicated platform, with strict access control and monitoring audits in place to ensure operational security.

- Account Management and Identity Authentication: A unified account management and identity authentication system are utilized for managing the lifecycle of employee accounts, ensuring each employee maintains a unique account. Password policies are enforced centrally; passwords are required to be robust and changed regularly, and multi-factor authentication is in play involving a dynamic verification code, obtained through the Tuya internal app, for secondary login verification.
- Authorization: Tuya grants limited resource access permissions to employees based on work positions and roles, adhering to the principles of least privilege and role separation. Employees request varying access rights via a centralized management platform subject to managerial approval, depending on work requirements.
- Monitoring: Tuya Cloud deploys an automated monitoring system for real-time, comprehensive monitoring of network devices, servers, databases, application clusters, and core operations running on the cloud platform. Metrics are displayed on multiple dashboards and alarm thresholds set for essential operational indicators with notifications sent out when these are exceeded.
- Auditing: All employee interactions with the production system are protocolled and must go through the bastion host. All operations are logged and sent in real time to a central log platform. Audit rules are defined for violations, triggering a notification to security personnel for follow-up in case of any violations.

10.1. Security Risk Management

The Tuya security team boasts a specialized team tasked with the management and identification of vulnerabilities, effectively enabling the discovery, tracking, investigation, and patching of security vulnerabilities.

Beyond the celebratory security penetration testing conducted before any business code is deployed online, Tuya also carries out intermittent penetration tests on its online

services.

Every year, Tuya engages third-party security firms to undertake penetration tests for services including but not limited to cloud services, mobile clients, and hardware products, stretching to encompass the entire Tuya IT framework.

Tuya encourages and rewards the contribution of external hackers (white hats) in revealing potential vulnerabilities through the Tuya SRC (https://src.tuya.com/) or other external communication channels by offering a maximum bounty of $100,000 for each quality high-risk vulnerability identified. Any vulnerabilities reported are verified and evaluated internally by Tuya before being tracked through a ticketing system for repair. Completion of repair and the details of the entire process are provided as feedback to the hacker.

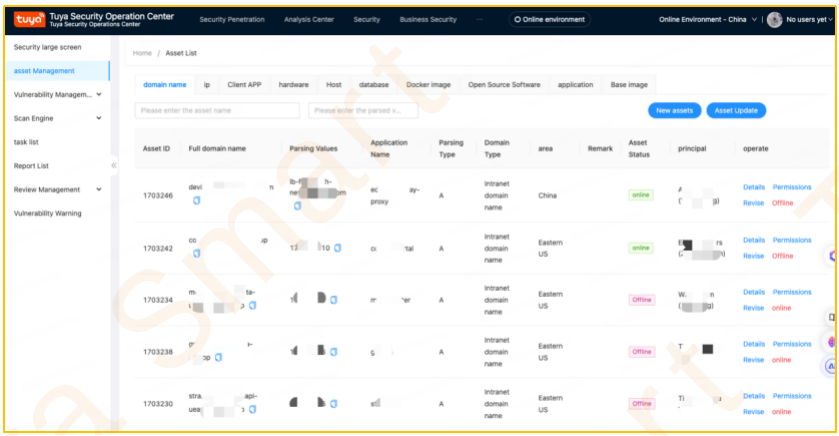
Vulnerability ratings are determined by a comprehensive evaluation encompassing factors such as the level of technical expertise required for the exploit, the scope of the impact, the difficulty in discovering and leveraging the vulnerability, the significance of the corresponding business operations, and potential damage caused by the vulnerability, all in accordance with 'Tuya's Vulnerability Risk Rating'. Internal vulnerability grading adheres to the standards established in CVSS3.1.

In the context of cloud vulnerabilities, the security team is mandated to confirm urgent vulnerabilities within 6 hours, followed by the development team rectifying the issue within 12 hours. High-risk vulnerabilities have a confirmation window of 1 day and a repair window of 2 days, while medium-risk vulnerabilities should be confirmed within 3 days and rectified within a week. The rectification timeline for low-risk vulnerabilities is assessed depending on business conditions. In scenarios involving apps and hardware, customers can refer to the vulnerability rectification timeframes stated in Tuya's SLA or similar documents.

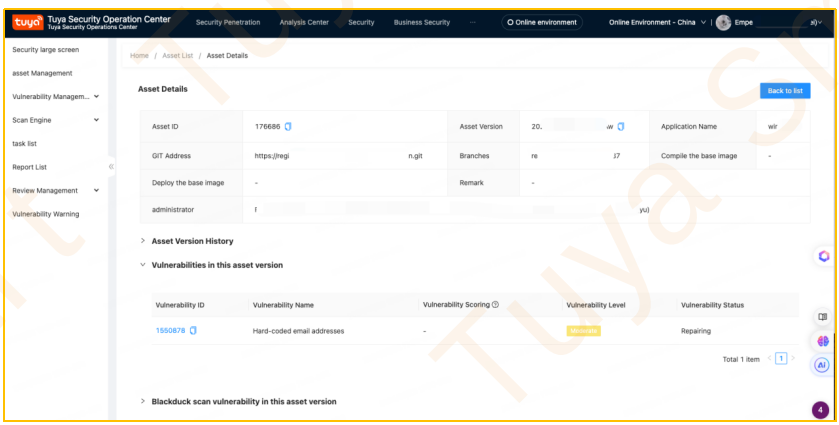
10.1.1. Asset Management

Tuya's approach to asset management employs a monitoring and managing procedure for security risks associated with assets and their versions, taking into account an attacker's point of view. Presently, the types of assets monitored include domain names,

IPs, client APPs, hardware, servers, databases, Docker images, open-source software, applications, and base images.



By carrying out continuous security tracking and vulnerability management, with versions relative to assets, Tuya is imbued with the means to quickly identify potential risks. Presently, Tuya ensures all types of assets are interlinked with security scanning tools, external threat intelligence platforms, and security testing evaluations. This aligns risks stringently with assets, while facilitating multidimensional and continuous monitoring of product and service assets under Tuya's ambit. This oversight allows an efficient response to security risks, creating a panoramic view of asset vulnerabilities for appropriate management.



10.1.2. Security Scanning

In an effort to fortify the security of the company's digital assets, we have established the following security scan timetable:

- Public network security scans: executed daily to enable prompt surveillance and expedited response to external threats.
- Online internal network security scans: conducted monthly to conduct in-depth audits of the internal network environment, identify, and pinpoint potential risks.
- Office network security scans: altered to a bi-weekly frequency to safeguard the security of data within the office environment and minimize potential attack vectors.

Utilizing a synergy of commercially available and open-source security scanning applications, our team is dedicated to the continual operation and optimization of scanning algorithms, ensuring they are updated in line with evolving network threats and are capable of effectively recognizing all categories of network vulnerabilities.

Upon completion of scanning, the results are promptly disseminated to relevant security operations personnel via enterprise WeChat. When a security vulnerability is detected, the system automatically tags the pertinent asset and version information on the platform, generating a nominated notification for the associated development team. The development team is mandated to immediately embark on vulnerability rectification, followed by submission to the security team for validation upon completion. Only upon confirmation from the security team that the vulnerability has been patched is the vulnerability status flagged as closed.

The Tuya security team remains vigilant in monitoring the network environment, adjusting the scanning strategy in accord with scan results, and emerging vulnerability trends, focusing efforts on high-risk areas.

10.1.3. Penetration Testing and Red-Blue Exercise

Penetration testing involves simulating plausible attack scenarios to assess security protocol efficacy. By mimicking hacker methodology, these tests attempt to bypass Tuya's security measures and attain the highest system permissions. The test's goals include identifying security vulnerabilities, confirming the validity of existing security

strategies, and determining the system's resilience against actual attacks. Moreover, Red-Blue Exercises, which simulate and practice real network attacks and defenses, aim to validate the security team's responsive capabilities and efficiency under real-world conditions.

Tuya's security team conducts a minimum of two internal Red-Blue Exercises annually, which challenges Tuya's personnel, organizational structure, and IT configuration. The exercise scope encompasses external network penetration, internal network penetration, and social engineering, among other elements. The purpose of these exercises is to promptly discover and fix flaws in security policies, thereby enhancing Tuya's overall protection capabilities.

To guarantee the objectivity and professionalism of these tests, Tuya ensures a minimum of two test instances conducted every year, entrusting renowned third-party security exchanges to conduct these penetration tests. Within the last three years, we have engaged with outfits such as Chaitin Technology, Anheng Information, CrowdSafe, Paloalto Network, Rapid7, Wizlynx Group, UnderDefense, ScienceSoft, and VTrust. These organizations perform extensive security evaluations and penetration tests on Tuya's cloud platform, apps, and hardware products, ensuring our services and products adhere to the highest security standards. Furthermore, through regular internal and external penetration testing, along with Red-Blue exercises, we continually refine and fortify Tuya's security framework.

We have set up the SRC (Security Response Center) and have publicly announced a bug bounty program. Our official website is: https://src.tuya.com. We sincerely encourage ethical hackers worldwide to report security concerns discovered within Tuya's products and services via this platform.

Moreover, Tuya has actively integrated multiple third-party crowdsourcing platforms to broaden the scope for vulnerability discovery and reporting. These platforms allow us to foster close collaborations with the global security research community, mutually striving to boost the security of Tuya's products and services. This open cooperation method not only endows us with a plethora of security viewpoints and solutions, but it also provides white-hat hackers a platform to showcase their expertise.

10.1.4. Security Incident Response

Tuya has established a comprehensive cybersecurity emergency response protocol internally to elevate the response capabilities to sudden cybersecurity incidents, mitigate

potential damages, and ensure the seamless operation of the company's business. This protocol aims to amplify emergency responsiveness, ensuring swift and effective actions when confronted with network-based threats.

For the security incident response process, we've implemented a strict categorization system for security incidents and vulnerabilities. Such a system confirms that we have apposite action plans corresponding to incidents of various levels. We have explicit steps and processes from the incident's discovery and detection, to containment, eradication, recovery, and post-incident analysis.

Our security incident management principle is 'proactive prevention, timely detection, rapid response, and assured recovery.' Under this principle, we've curated a detailed security incident management flowchart. In this flowchart:

- The purple line signifies the 'top-down' response process, primarily initiated by the higher security departments with security announcements as the initiation point;
- The blue line indicates the 'bottom-up' procedure, typically initiated by monitoring personnel or system maintenance team, commencing from the discovery of security incidents by security monitoring or information security operational and maintenance personnel;
- Brown represents circumstances where the 'non-emergency security incident process' is invoked, mainly initiated by security monitoring staff.

This robust emergency handling protocol and process workflow ensure that Tuya can react quickly and systematically when confronted with cybersecurity incidents, drastically mitigating potential detriments, and safeguarding the continuous and stable operation of the company's business.

In instances where a customer's business stability and security are impacted, Tuya also provides them with a detailed investigation report. When required, we follow legal and regulatory guidelines to report vulnerabilities to regulatory bodies, and take necessary steps for public vulnerability disclosure.

10.1.5. Security risk Assessment

To select the appropriate control objectives and mechanisms whilst contemplating a

balance between control costs and risks, and to make sure information security risks are at a manageable level, Tuya conducts a thorough risk assessment at least annually.

Our security risk assessment strategy is intrinsically linked with the company's overall security control approach and procedures, simultaneously ensuring compatibility with international mainstream standards for its effectiveness.

Throughout the evaluation process, we construct a global modelling view for Tuya's existing services. This assists us in deeply analysing potential threats present within the internal mechanisms of the system. Concurrently, it enables us to identify any abnormal and detrimental behaviour that could emerge during the system's interaction with the external environment. These analyses allow us to accurately pinpoint the system's weaknesses and the security threats it faces, thereby implementing effective measures to reduce and manage risks.

10.1.6. Security Audit

To ascertain transparency and traceability in security management, the Tuya security team enforces rigorous audit measures across all key processes. This includes access to platforms and tools involved in the security framework, configuration alterations, and permission granting. Every operation's details are extensively logged, thus ensuring the preservation of all audit records for any future reviews and analyses.

To further fortify our auditing capabilities, we've established an innovative internal security audit platform. This platform is successfully integrated with the core management system within the company, allowing for a unified, centralised auditing of all employee access and operational logs. With this platform, we can monitor and analyse various operational behaviours in real time, facilitating prompt detection of potential security risks or anomalous behaviours.

Furthermore, the security audit platform employs a host of technical methods to guarantee the accuracy, completeness, and non-repudiation of audit logs. Signifying all audit records are securely encrypted and stored to avert any unauthorized tampering or deletion, thus reinforcing the high credibility and the legal binding nature of audit data. Through these initiatives, Tuya establishes a robust security auditing framework,

providing substantial support to the company's information security.

10.2. Employee Permissions and Access Control

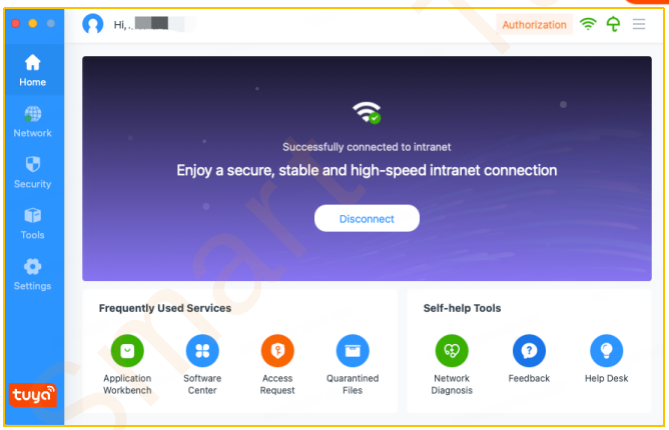
Tuya incorporates a cohesive management approach for different types of permissions within the IT framework, comprising network, system, machine, and data permissions, successfully establishing a zero-trust permission management model.

With this model, we administer detailed identification and authentication influenced by several factors like network admission, user identity, application identity, and application functionalities. By doing so, we can definitively assure that each user or application only attains the minimal required permissions, effectively forestalling permissions abuse and potential security risks.

Furthermore, we employ cutting-edge permission control techniques and tools to ensure the allocation, modification, and revocation of permissions undergo strict supervision and auditing. Not only bolstering the transparency and efficiency of permissions management but also significantly elevating Tuya's holistic information security levels.

10.2.1. Zero-Trust Secure Access in the Office Network

Tuya harnesses an SASE zero-trust network policy to supersede VPN connections, transitioning the entire office network into a digital platform. Regardless of location - home, office, or anywhere else, employees are bestowed access permissions factoring in their user identity, geographical location, terminal device status, and terminal security status. This strategy supports employees with secure and convenient working conditions at any time, in any place. The implementation of this zero-trust model has enabled us to establish an enterprise security boundary consisting of trustworthy individuals, reliable terminals, and secure devices.

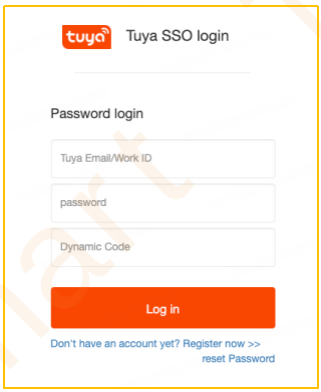


10.2.2. Internal System Permission Management (AAA)

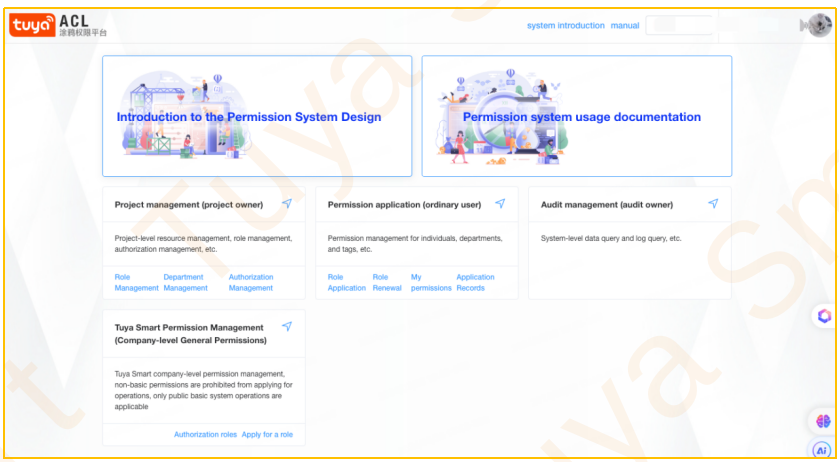
Tuya exercises stringent supervision over system permissions management, encompassing a wide array of elements including internal system platform permissions, application permissions, machine permissions and so forth. When authorizing system permissions, we stringently adhere to the "least privilege principle". Consequently, each permission role is assigned the bare minimum permissions required to accomplish its tasks or operations, circumventing surplus permissions and potential security vulnerabilities.

To safeguard the transparency and traceability of permission management, the system meticulously records an audit trail for all permission modifications. These logs encapsulate all permissions' allocation, alteration, and revocation, thereby presenting an available resource for the security team to review and analyze.

For identity verification in internal systems, Tuya employs state-of-the-art Single Sign-On technology (SSO). This technique extensively simplifies the login process for employees, improving operational efficiency while bolstering identity verification security. Furthermore, our SSO system has integrated an OTP (One-Time Password) function, ensuring that employees input a dynamically generated verification code each time they log in, thereby elevating the security of identity verification even further.



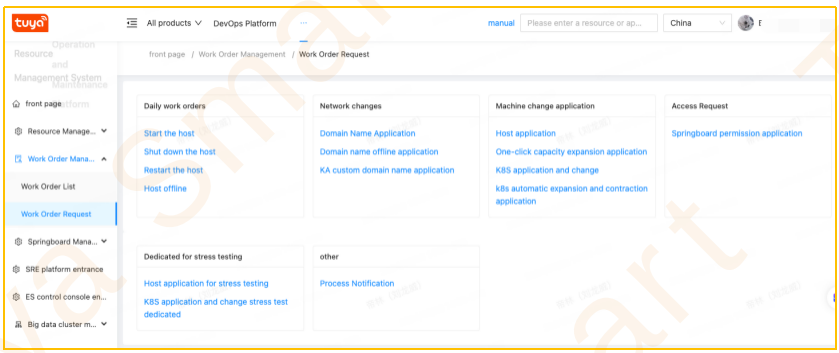
For internal system permission validation, we've instituted a standardized permission management system (ACL). This system has the capability to adeptly delegate permissions for applications, application functionalities, and data. Leveraging this system, we can comfortably oversee and manage the access permissions of various users or roles encompassing a broad spectrum of resources and data. Additionally, the platform features a thorough approval process management function, ensuring all permission alterations undergo rigid reviews and approvals.



Collectively, these strategies contribute to Tuya's holistic and intensive system permission management approach, establishing robust security measures for the company's information security.

10.2.3. Machine Permission Management

At Tuya, we have implemented stringent and consistent management over the application and approval process for machine permissions by our staff. To bolster the rationale and security of permission allocations, we've established a dedicated platform for processing machine permission applications from employees.



Within this process, the initial step mandates employees to submit an application to their immediate supervisor, outlining the reasoning and scope underlying the request for permissions. Subsequently, the supervisor conducts a preliminary evaluation of the request, confirming its justification and necessity. Thereafter, the applications are escalated to the operations and maintenance, security, and application heads for approval, sequentially. These appraisers meticulously review the application in congruence with the company's security policies and best practices.

Following all necessary approvals, the permissions are formally disseminated. Post-authorization, employees can manage limited machine permissions by logging into the bastion host. The bastion host is a state-of-the-art device designed to facilitate secure remote access, ensuring operations by the staff are only within their authorized clearance, consequently mitigating unauthorized access and associated security risks.

Simultaneously, to guarantee the integrity and traceability of audits, we maintain detailed records and conduct audits encompassing the entire permission approval workflow, machine login sessions, executions of commands, and file transfers among others. These audit trails are securely preserved in robust storage facilities for potential future analyses and reviews. With these measures in place, we can promptly identify and address any potential security issues or anomalous behavior, thereby comprehensively safeguarding the company's information security.

10.2.4. Application Permission Management

Tuya spearheads comprehensive and granular control over individual applications and the communication permissions between them, facilitating centralization and precision in permission management. To accomplish this, we stipulate the use of a standardized Client component for all service access within Tuya’s internal applications.

While this unified Client component enables service access, it also substantiates mutual recognition of user identities and empowers regulation of their permissions. Harnessing this component, we can certify every user is accurately identified and authenticated during their application access, permitting or restricting them from performing unique operations contingent on their roles and permissions.

Additionally, we've developed a unified authentication service to manage authentication requests across all applications. This service, premised on preset permission guidelines and rules, validates and authorizes every user's access request. The authentication service grants access to relevant applications or resources only when users possess the

requisite permissions for specific tasks.

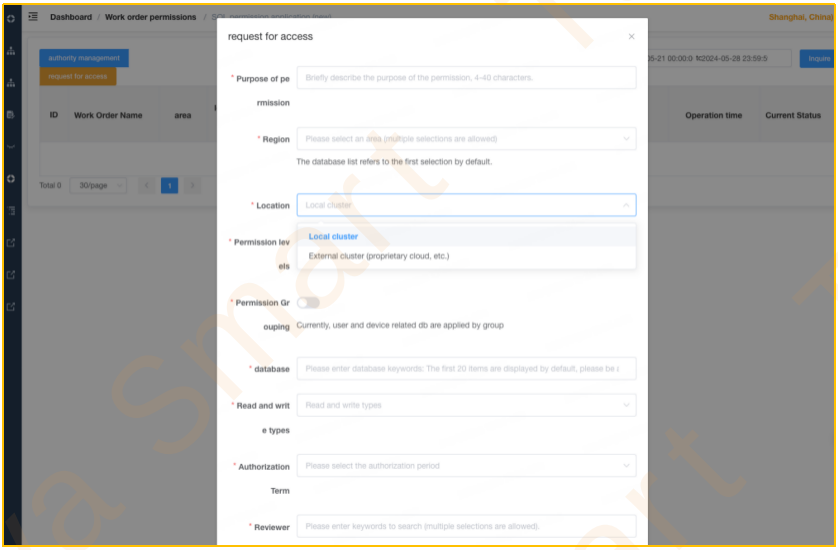
These safeguards assure the consistency and security of internal application service access and permission controls within Tuya. This strategy effectively counters unauthorized access and potential security vulnerabilities, securing the company's critical data and resources.

10.2.5. Database Permission Management

At Tuya, we maintain diligent database permission management, primarily addressing the administration of application and database platform accounts.

In terms of application accounts, these are particularly provisioned for application programs to facilitate database access. These accounts, correlated with the machine identifiers of their associated applications, authenticate identities and ensuring only authorized applications can gain access, thereby thwarting unauthorized access and potential security risks.

Concerning database platform accounts, we implement more rigorous management. These accounts are created and managed specifically by our Database Administrators (DBAs) that certifies their security and compliance. Depending on the account's purpose and access requirements, we create various account types like read/write accounts for dispatching work orders and read-only accounts solely for querying modules amongst others. To bolster the security of these database platforms accounts, we institute a rotational policy every three months, mitigating the risk of password breaches and account abuse.



For databases that contain user or sensitive personal information, we enforce more stringent permission management measures. We restrict the account volume for such databases and maintain a strict control over the long-term and temporary permissions. For further assurance, specific data centers can employ even tighter controls based on their specific needs, ensuring the security and privacy of user data.

Other business databases adhere to a standardized access control policy, setting a maximum limit on the quantity of accounts each database can have, inclusive of long-term, mid-term, and temporary accounts. This approach ensures each account's permissions align suitably with its actual necessities, thwarting potential permission misuse and security risks.

To monitor and assess the compliance and security of database access, we conduct bi-annual database access audits. The first stage of these audits is executed by the DBA, performing a comprehensive analysis of database access logs and operation records to identify any anomalous behavior or potential security issues. The compliance department serves as a secondary reviewer, cross-verifying the audit findings to guarantee the precision and reliability of the audit results. By deploying these audit processes, we can promptly detect and handle potential security threats or infringements, comprehensively

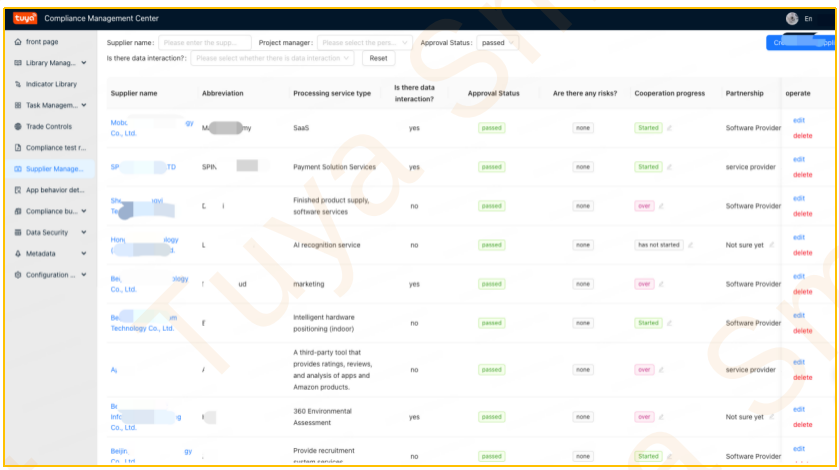
safeguarding our company's database security.

10.3. Supplier Relationship Security Management

10.3.1. Supplier Assessment

Tuya maintains stringent supplier admission management over our platform software vendors. At contractual and delivery stages, our security and compliance team comprehensively evaluate the supplier's contracts, products, and services. Moreover, we conduct at least an annual reassessment to ensure the supplier's continued compliance and security.

Besides analysing the product's security metrics and the security standards of software services, Tuya seeks a thorough understanding of each service provider's practices in information security assessments and privacy compliance. For information security assessment, we consider various aspects such as security penetration testing and supplier security capability assessments to ensure that the supplier's security abilities align with our requisites.



Simultaneously, we place high priority on assessments related to data security and privacy compliance. The specific evaluation standards and methodology can be found in section 6.4. This section elaborates in depth on the assessment standards and processes for data security and privacy compliance, thereby ensuring consistency and precision in our evaluation process.

Via these measures, Tuya ensures that our collaboration with suppliers is secure and compliant, providing a robust safeguard for the company's sustained growth.

10.3.2. Quality of Supplier Services Monitoring

Tuya proactively regulates the quality of supplier services in real-time, staying vigilant to the supplier's security updates and developments. We've instituted an intricate monitoring mechanism and response procedure to ensure immediate reaction in case of any abnormality.

Particularly, we employ various monitoring tools and techniques to supervise the quality of supplier services in real-time, comprising aspects like system performance, network connectivity, and service availability. Concurrently, we maintain open channels of communication with suppliers, allowing us to promptly understand their security updates, thereby acting swiftly upon any emerging security incidents or vulnerabilities.

Upon detecting anomalous activities, our security team will instantaneously enact the emergency response protocol, swiftly identify, analyse, and address the event. We will work hand in hand with the supplier, coordinating resources and technical support to restore the normal functionality of services in the minimum possible time and avoiding such incidents in the future.

By employing these strategies, Tuya ensures continuous vigilance and high response capabilities during its collaboration with suppliers and safeguards the continuity and security of the company's business operations.

10.4. Customer Security Service Support

Tuya's products and services come equipped with comprehensive operational security capabilities, providing customers with 24/7 technical support and ensuring that customers enjoy continuous, reliable, and secure services throughout their use of Tuya's offerings.

Our technical team possesses extensive experience and technical expertise, enabling them to respond quickly and resolve any issues customers may encounter during use. Whether it's system malfunctions, network problems, or security incidents, we are ready to provide effective technical support and solutions immediately.

Furthermore, we have established a comprehensive monitoring and early warning mechanism to conduct real-time monitoring and analysis of our products and services. This allows us to promptly detect and address potential security risks and hidden faults, thereby ensuring maximum protection for our customers' business continuity and data security.

Additionally, we conduct regular security vulnerability scanning and perform security hardening measures to enhance the overall security of our products and services.

In summary, through our comprehensive operational security capabilities and around-the-clock technical support, Tuya is committed to delivering an efficient, stable, and secure IoT service experience to our customers.

11. Business Sustainability

11.1. Business Continuity

Tuya is well aware of the potential significant losses that a disruption in key production and business activities, major faults, or disasters can cause to any enterprise. To ensure business continuity and stability, we conduct 24-hour continuous real-time monitoring of all hosts, applications, services, and networks on our cloud platform through our operational and maintenance platform. This platform is equipped with a complete set of automated business fault handling procedures and support systems, enabling a swift response to failures and ensuring zero service interruption for users through a multi-service hot-swapping mechanism.

Taking into account risks posed by uncontrollable factors such as business system software or hardware failures, as well as natural disasters, we have devised a comprehensive and effective contingency plan. In foreseeable circumstances, we are capable of ensuring the continuous and stable operation of the business, minimizing potential losses to the greatest extent possible.

11.2. Disaster Recovery

Data security is the lifeblood of any enterprise. To guarantee the security, reliability, and continuous availability of business data, we have implemented multiple safeguards, including real-time hot backups of primary and replica data, redundant storage, and geographical backups. This means that even in extreme situations, we are able to quickly restore data, thereby ensuring business continuity.

Additionally, we continuously monitor and verify backup status to ensure accurate and complete data recovery at all times. For our business system, we have deployed multiple failover systems to address potential network failures or other unexpected events, ensuring fast and seamless emergency switches during critical moments.

11.3. Emergency Response Plan

Inside Tuya, we have developed comprehensive emergency response plans tailored to diverse types of assets and security risks. These plans are based on the "Tuya Smart IT

Emergency Process Guidelines" and aim to ensure prompt, organized, and efficient emergency response in the event of an unexpected incident, thereby safeguarding the smooth operation of the company.

The emergency response plan encompasses various components, including preemptive plan formulation, system monitoring, and a range of troubleshooting methods. During an incident, our comprehensive system monitoring and audit logs provide ample data support for subsequent analyses. Additionally, we have designated points of contact for different emergency scenarios to ensure seamless information exchange. After the incident, we follow a comprehensive response process and emergency plan to quickly resolve issues, investigate root causes, and determine accountability.

11.4. Emergency Drills

To continuously improve our emergency response capabilities, Tuya regularly conducts extensive internal technical emergency drills and simulations of real-life situations. These drills cover multiple aspects, such as hardware failure simulations, defending against network DDoS attacks, and managing security events. Through these exercises, we are not only able to verify the effectiveness and feasibility of our existing emergency plans, but we can also identify potential issues in a timely manner and continuously refine and optimize our response strategies.