涂鸦智能安全白皮书

Tuya Smart Information Security White Paper

Version 4.1.

Catalog

目录

1. 涂鸦智能介绍

涂鸦智能是一个全球化智能平台，“AI+IoT”开发者平台，也是世界排名前列的语音 AI 交互平台，连接消费者、制造品牌、OEM 厂商和零售连锁的智能化需求，为客户提供一站式人工智能物联网的解决方案，并且涵盖了硬件接入、云服务以及 APP 软件开发三方面，形成人工智能+制造业的服务闭环，为消费类 IoT 智能设备提供 B 端技术及商业模式升级服务，从而满足消费者对硬件产品更高的诉求。

截至 2021 年 3 月 31 日，涂鸦 IoT 开发平台累计有超过 32.4 万注册开发者，日语音 AI 交互超 1.22 亿次，每日设备请求次数 840 亿次，Powered by Tuya 赋能超 31 万设备 SKUs，产品和服务覆盖超过 220 个国家和地区，辐射全球超 10 万个线上和线下销售渠道。。

1.1 涂鸦云平台介绍

涂鸦智能在全球范围内部署云服务，致力于为全球客户提供安全、稳定、快速的云服务。涂鸦云平台拥有亿级海量数据并发处理能力，为用户提供稳定性高达 99.99% 的不间断计算服务。涂鸦整合了不同云平台的全球服务节点，为全球各区域用户提供就近的访问服务，保障高效稳定的设备使用体验。云平台提供了从产品定义、模拟测试、硬件开发、客户端开发、云平台交互、产品测试、运行管理、数据分析等覆盖智能硬件接入到客户端控制全生命周期

的服务能力。

涂鸦云平台为创客和厂商提供了自助式软硬件开发 SDK 与开放完善的云平台 API，同时提供调试助手，降低了硬件厂商的开发门槛，提升智能产品的投产速度。同时，云平台还能帮助厂商进行软硬件智能升级，持续为消费者提供优质的智能服务。

1.2 信息安全保障的使命

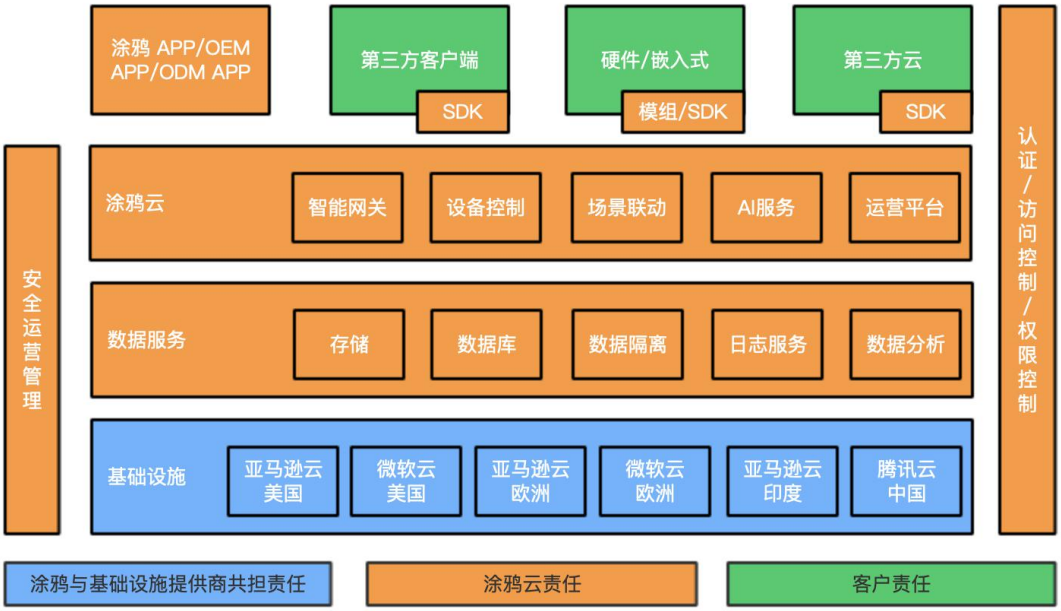
涂鸦致力于为客户提供一致、可靠、安全和符合法规要求的 IoT 接入服务，切实地保障客户及其用户的数据的可用性、机密性和完整性。涂鸦云承诺：涂鸦云以数据保护为核心，以云安全能力为基石，依托涂鸦独有的物联网解决方案，打造业界领先的竞争力，构建完善的云平台安全保障体系，并一以贯之的将信息安全保障作为涂鸦云的重要发展战略之一。

为了达到这些目标，涂鸦实现了各个层面的安全防护包括对外所有服务的安全检查、安全防御以及安全监控和审计，形成事前、事中、事后的全过程防护。

该白皮书致力于让客户更加全面、系统的了解涂鸦，并对涂鸦云平台有更深入的安全洞察。

2. 安全责任

涂鸦负责涂鸦云平台上的服务和数据交互的安全管理和运营，对提供的云服务平台和基础架构的安全性负责。客户自行开发 APP 或硬件嵌入式软件(包括使用 SDK)接入涂鸦云需要客户自己保障其应用及数据（详见 2.2 条），包括硬件和 app 的安全合规。下图为基础云服务商、涂鸦以及客户信息安全责任共同承担责任模型：



2.1 涂鸦云的安全责任

涂鸦云通过选择全球知名的云主机服务商亚马逊、微软云和腾讯云等全球一流云计算平台，确保安全管理和运营的基础设施，物理设备的安全。

涂鸦云安全覆盖数据安全和云服务安全。涂鸦承诺利用其安全团队以及全球范围内知名的安全服务厂商的专业攻击防护技术经验，提供云平台的安全运维和运营服务，切实保护涂鸦云的安全运营，以及保障客户、用户隐私和数据的安全。主要覆盖但不限于如下：

- 数据安全：指客户在云计算环境中的业务数据自身的安全管理，包括收集与识别、分类与分级、权限与加密以及隐私合规等方面；
- 访问控制管理：对资源和数据的访问权限管理，包括用户管理、权限管理、身份验证等；
- 云服务安全：指在云计算环境下的业务相关应用系统的安全管理，包括应用和服务接口的设计、开发、发布、配置和使用等方面。

2.2 客户的安全责任

客户在使用涂鸦云的解决方案的时候，需要严格按照涂鸦的安全配置和接入要求执行。同时客户需要保证自己的云端、客户端或者硬件产品本身的安全性。基于涂鸦 SDK 开发的 APP，涂鸦仅提供技术支持，但是无法提供任何安全保障。对于基于涂鸦 OEM(公版)APP(无任何定制场景)的数据安全合规、隐私政策等相关信息，涂鸦会提供模板供客户参考，具体上线的隐私政策声明以及法律合规性由客户自己负责，必要时候，涂鸦安全团队愿意提供安全解决方案的帮助和咨询服务。

3. 合规产品与认证

涂鸦遵守国际权威的安全标准及行业要求，并整合到内部控制框架中，在云平台、APP、硬件产品等需求实现过程中严格执行。涂鸦是中国家用电器协会、智能家电云云互联互通工作组成员、智能家电云云互联互通工作组-安全组的组长单位，牵头制定了中国智能家居云云互联互通信息安全标准。涂鸦参与了全国智能建筑及居住区数字化标准化技术委员会的智能家电信息安全标准的撰写。涂鸦还参与中国通信标准化协会，并参与了相关的物联网标准的制定和撰写。

同时，涂鸦还与独立第三方安全服务、咨询和审计机构进行合作，验证和保障了涂鸦云平台的合规性和安全性。

目前，涂鸦已经通过全球多个咨询和审计机构的信息安全和隐私合规的认证，是一家拥有多个认证的 IoT 解决方案提供商。涂鸦承诺，将持续地进行多个信息安全和隐私安全相关的认证和合规证明，为客户的数据和隐私安全保驾护航。

目前，我们的认证和合规凭证如下所示：

3.1 ISO/IEC 27001

ISO/IEC 27001 是信息安全管理体系（ISMS）国际标准，为各类组织建立并运行信息安全管理体系提供了最佳实践指导。按照标准要求：

- 基于业务风险的方法，建立、实施、运行、监控、评审、维护和改进信息安全；
- 为了确保信息的机密性、完整性和可用性，设立了相应的组织架构，建立了体系化的安全管理制度，并提供资源保障；
- 遵循 PDCA 方法，持续改进信息安全管理。

3.2 ISO/IEC 27017

ISO/IEC 27017 为云计算的信息安全方面提供了指导，推荐实施专门针对云的信息安全控制，从而对 ISO/IEC 27002 和 ISO/IEC 27001 标准的指导做出补充。此实施规程针对云服务提供商提供了更多信息安全控制实施指导。

涂鸦云经过多年的努力，大力推进 ISO/IEC 27017 的落地，不仅表明了我们会始终采用国际公认的最佳实践，也证明了涂鸦云平台拥有专用于云服务的高精度控制系统。

3.3 ISO/IEC 27701

涂鸦云获得了 ISO/IEC 27701 隐私安全认证，进一步印证了涂鸦在国际隐私权和数据保护标准方面的承诺。

ISO/IEC 27701 隐私信息管理为 ISO/IEC 27001 信息安全管理系统和 ISO/IEC 27002 安全控制的隐私扩展。它是一项国际管理系统标准体系，为保护个人隐私提供指导，包括组织应如何管理个人信息，并协助证明遵守了世界各地的隐私法规。

着重隐私保护的控制措施，定义管理流程并提供持续发展的基础上保护 PII（个人可识别信息）的实务指南。同时整合 ISO27001、ISO27001 和 ISO29100 的最佳实践。是目前相关标准中最新公布的版本，并与隐私保护议题高度接轨。

3.4 CSA STAR

确保 IT 网络与数据安全对企业而言至关重要。STAR 云安全评估是一个全新而独特的服务，旨在应对与云安全相关的特定问题，是 ISO/IEC 27001 的增强版本。为了应对与日俱增的商业问题，云安全联盟（简称为 CSA，这是一家非盈利性组织，其使命在于推广云计算方面的最佳实践）开发并推出了云控制矩阵（CCM）。该矩阵由一个行业工作组共同开发，规定了云安全相关的常用控制措施。

涂鸦参与 STAR 云评估安全项目，使得涂鸦在云安全管理体系达到国际标准与云安全行业预期的进程上，迈出了重要的一步。

3.5 ISO 9001

涂鸦智能已获得 ISO 9001 认证。

ISO 9001 是由全球第一个质量管理体系标准 BS 5750（BSI 撰写）转化而来的，ISO 9001 是迄今为止世界上较为成熟的质量框架。它是一个系统性的保证公司产品质量及运作的指导性纲领和规范架构，围绕企业提供的产品或服务展开。策划和实施及改进产品或服务实现的

全过程，确保满足客户及相关法律法规要求。

运用质量管理系统，能够有效和高效地实现预期的质量目标。通过对质量管理体系的审核和管理评审，采取纠正措施和预防措施。持续改进质量管理体系的有效性，是企业发展与成长的根本。

3.6 GDPR

欧盟的通用数据保护条例（GDPR）旨在保护欧盟及欧洲经济区数据主体的基本隐私权和个人数据安全。它提出了更为严苛的保护标准和要求，并设置了高昂的违约成本，大大提高企业在对欧盟公民信息处理及保护方面的安全性、合规性标准及成本。

目前，涂鸦已经获得 TrustArc 的 GDPR 合规验证报告。通过与 TrustArc 建立合作关系，对 GDPR 要求进行严格合规剖析并审核。利用 TrustArc 科学定制的合规审核平台，按照一整套安全合规流程提供工具和解决方案，及时评估准备情况，制定并执行 GDPR 合规计划。TrustArc 将每年持续为涂鸦建立，实施和演示方法帮助管理和维护的 GDPR 合规。

3.7 CCPA

涂鸦智能已获得 Trustarc 的 CCPA 合规验证报告。。

加州消费者隐私法案(CCPA)已于 2020 年 1 月 1 日正式生效，旨在加强消费者隐私权和数据安全保护，CCPA 被认为是美国国内最严格的隐私立法。

在与 TrustArc 的战略合作中，涂鸦评估审核并认证了多项合规与体系建设，并在数据隐私及评估等安全方面不断优化升级，表现出行业领先的高水平且成熟的完备机制。

3.8 EPC - TRUSTe 企业隐私认证

涂鸦经过一年准备，正式通过 TrustArc 的企业隐私认证，并获得隐私认证标志，证明涂鸦充分实施了隐私政策和隐私相关控制，涂鸦的隐私和企业数据管理在整体合规框架中上升到了更为成熟的阶段。

3.9 AICPA SOC2 TypeII 审计报告

由美国注册会计师协会颁布标准，SOC2 TypeII 是数据安全领域的一项权威认证，用于确保服务供应商安全地管理数据，保护企业利益及其客户隐私。涂鸦顺利通过 SOC2 审计证明了涂鸦在保护客户隐私和数据安全领域已达到领先水平。

3.10 等级保护测评三级

通过等级保护测评意味着涂鸦智能满足《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》第三级对应的安全指标要求，满足在涂鸦云上客户的信息系统在等级保护三级合规相应的技术和管理要求。

3.11 ETSI EN 303645

ETSI EN 303645 是欧盟发布的消费电子 IoT 产品安全技术标准，该技术标准主要规定消费类物联网产品及其相关服务的网络安全，同时也将部分商用物联网产品纳入标准范围。旨在为消费类物联网产品建立安全防线，保障用户隐私。能够帮助物联网产品符合设计安全要求

准则，支持全球物联网产品网络安全和欧洲 GDPR 合规。目前英国目前正在推进的物联网法也是基于该标准的技术要求。

Product Service

涂鸦智能 WBR3（WIFI+BLE 双模）模组通过了 TUV SUD 的 ETSI EN 303645 测评和认证，表明涂鸦在 WIFI 和 BLE 的软件安全和协议安全等符合了欧盟对消费电子 IoT 产品安全技术标准，也满足了 GDPR 的用户数据保护法规。该认证的获取，表明了涂鸦的产品线，不管是涂鸦云，涂鸦智能移动终端，还是涂鸦智能的模组产品，都获得了第三方的 GDPR 背书。未来，涂鸦智能将继续探索和研发更加安全的产品和服务。

3.12 “智能硬件(IoT)开放平台”的测试评估

涂鸦智能凭借涂鸦全球化“物联网+”平台，通过了“智能硬件（IoT）开放平台”认证测试，获中国信息通信研究院和移动智能终端技术创新与产业联盟颁发可信硬件（IoT）认证。涂鸦在平台的开放性、安全性、稳定性、平台处理设备连接的并发性能等各方面均受到了认可。

工信部指导的智能硬件（IoT）可信评估旨在推进智能硬件（IoT）终端研发与云服务提供的标准化与规范化，促进互联互通和产品成熟，对参评云平台的数据存储可靠性、用户数据私密性、功能完备性、运维系统完善性等云服务能力有严苛的量度与测评。

3.13 其他合规

涂鸦内部有专门的隐私合规团队，紧密跟踪行业动态，第一时间跟进全球范围内的主要安全和隐私合规标准，和各个国家的信息安全和隐私保护相关的法律，并通过第三方安全服务机构和隐私保护相关律所机构合作，实时审核验证涂鸦的业务合规情况。近几年包括俄罗斯、印度国家等用户数据保护法律，包括英国、美国加州和美国华盛顿州的 IoT 相关的法案，包括欧盟官方推荐的信息安全实践标准等，涂鸦都进行了严格的内部审计和风险评估，确保所有涂鸦的服务和产品都能够满足这些要求。

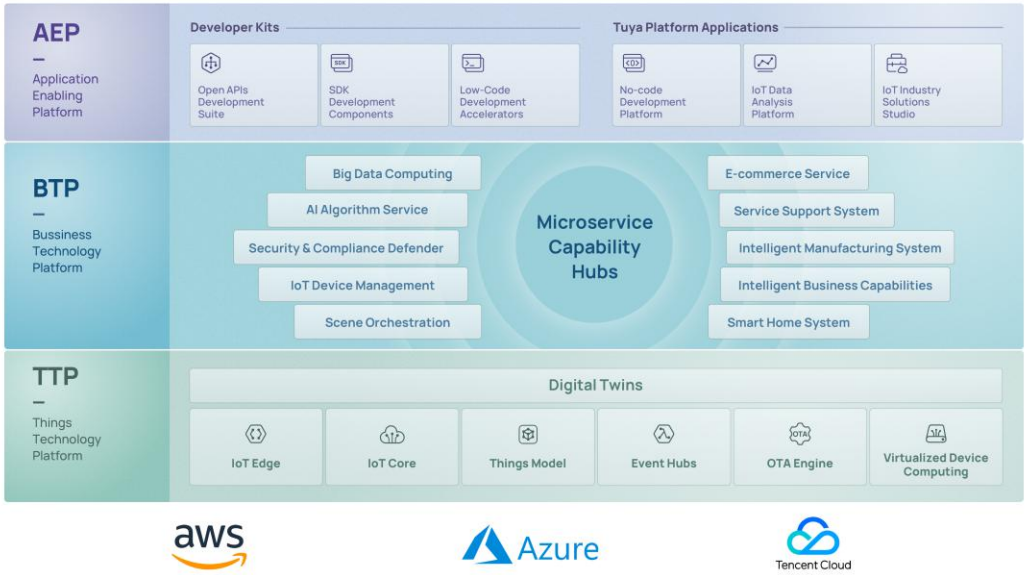
目前涂鸦也在进行其他的认证审计，未来将会有更多权威的第三方审计和认证报告能够呈现给客户。

3.14 合规内审

为保证公司信息安全管理体系和隐私合规体系持续有效运行，涂鸦有专门的合规管控人员，每年至少执行一次内审，会对企业组织的内控、合规管理和风险管理进行检查监督和评价，其中会审计验证本公司有关信息安全管理活动是否符合 ISO/IEC27001:2013、ISO/IEC27017:2015、ISO/IEC27701:2019、CSA Star 云安全认证、AICPA SOC2 等标准的要求、是否符合 GDPR、CCPA 等相关法律法规的要求、是否符合新版信息安全管理体系的规定以及信息安全管理体系的有效性，并根据具体不合规的点，进行整改推进。

4. 云平台基础架构

4.1 云平台基础架构图



涂鸦云平台的基础设施由 AWS、Azure、腾讯云等提供，整合了全球服务节点。在平台定义层面，提供了从产品定义、模拟测试、硬件开发、客户端开发、云云平台交互、产品测试、运行管理及数据分析等覆盖智能硬件接入到运行全生命周期的服务能力。在服务层面，为创客和厂商提供了自助式软硬件开发 SDK 与开放完善的云平台 API。

详细的云平台接入开发文档，详见：https://docs.tuya.com/zh/iot。

4.2 云服务器供应商要求

涂鸦云选择云服务器供应商要求：

1. 全球知名云服务提供商品牌，技术水平全球领先。

2. 云计算产品安全和稳定。

3. 拥有和符合全球范围内最完备的信息安全合规、法律和资质证明。

目前被我们选择的云服务器提供商，包括 Amazon、Azure、腾讯云。

5. 数据安全与隐私保护

5.1 涂鸦云数据安全体系

涂鸦践行“一切以用户价值为依归”的经营理念，尤其重视与客户建立长久持续的信任关系。云数据安全体系从数据安全生命周期角度出发，采取管理和技术两方面的手段，进行全面、系统的建设。通过对数据生命周期（数据收集、存储、加工、传输、共享、删除）各环节进行数据安全管理管控，实现数据安全目标。

在数据安全生命周期的每一个阶段，都有相应的安全管理制度以及安全技术保障。

5.2 数据所有权

涂鸦致力于个人隐私保护，因此遵照所有的数据保护法规定，数据的归属权和所有权均属于个人用户。而相对来说，涂鸦为客户定制的服务中，客户是数据控制者，客户有权利决定数据的使用方式和目的，但与此同时，客户需要保证数据使用的合规性；涂鸦是数据处理者，涂鸦将在符合法律法规的基础上按照客户书面指示、合同约定来处理客户个人数据，所有数

据处理行为对客户透明。因此，在符合数据保护的法律法规、《涂鸦隐私政策》的基础上，涂鸦可帮助客户和用户保障数据的保密性、完整性、安全性。

5.3 数据生命周期安全管理

5.3.1 数据安全和隐私保护基本原则

涂鸦的产品和服务开展个人数据处理活动，遵循以下基本原则：

1） 权责一致原则——对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

2） 目的明确原则——具有合法、正当、必要、明确的个人信息处理目的。

3） 选择同意原则——向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意。

4） 最少够用原则，即数据最小化原则——除与个人信息主体另有约定外，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量，不收集、存储、请求、提供、传递与服务无关的数据。目的达成后，应及时根据约定删除个人信息。

5） 公开透明原则——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。

6） 确保安全原则——具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

7） 主体参与原则——向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户等方法。

5.3.2 个人隐私权益保障

当今数据安全和隐私保护法律法规强调保障个人隐私权益，涂鸦内部形成了《个人权利处理流程》，在提供服务的基础上最大程度保障用户个人权利的实现。于此同时，涂鸦也为客户在响应用户隐请求时提供帮助，具体包括以下个人权限：

1) 保障用户知情权

- APP 和网站的隐私政策，具体可查看 https://auth.tuya.com/privacy?from=http%3A%2F%2Fiot.tuya.com%2F
  - ✓ 隐私条款必须明确应用收集的所有用户数据类型及与之相对应的服务。
  - ✓ 隐私条款在涉及用户账号注册时需要通过邮件、APP 弹窗等方式告知用户，与此同时，涉及内容上的重大变更时，如涉及新的数据类型的收集，收集个人敏感类数据，使用数据用于新的用途时，该版本隐私协议需要用户的明确授权才能急需提供服务。
- 网站 Cookie 声明
  - ✓ Cookie 的作用及用户选择权。

2) 访问权

涂鸦用户可通过 App 访问涂鸦收集的个人数据，无需另外技术支持。

涂鸦用户可请求涂鸦告知对其数据的处理和使用情况，

3) 被遗忘权（数据删除权）

用户作为数据的所有者，可以通过 APP 上的账号注销功能或提交反馈/联系官网客服的方式

对数据做完全的删除。 删除的数据包括但不限于用户身份信息、用户对于 APP 和智能设备的使用记录，智能设备在用户使用期间所产生和收集的信息等。

4) 纠正权

若得知用户主动提供的个人信息存在不准确或需及时更新的情况，用户可在 App 上手动修改。

5) 可携带权

用户通过涂鸦 APP 反馈或者客户邮箱反馈，要求将提供给涂鸦的个人数据传输给另一个数据控制者。

5.3.3 数据生命周期安全管理

1) 数据收集

涂鸦秉承数据保护的基本原则以及保障个人隐私权利前提下进行数据收集。用户对于数据收集的同意是我们最主要的法律依据，通过保障用户的知情权，以及服务的必要原则而进行数据收集。

2) 数据存储

- 数据与文件存储安全

涂鸦云会对企业数据进行隔离，保障客户数据的安全性。同时涂鸦云针对不同的业务场景提供不同的数据存储服务对客户或用户的敏感数据使用 AES256 进行加密存储，部分敏感数据会进行必要的脱敏处理，同时密钥通过密钥管理中心进行统一的安全管理和分发。

对于用户敏感媒体类型信息，比如图像或录像等文件，涂鸦基于特定用户和特定设备生成唯一的密钥对文件进行加密保护。

- 数据存储区域

六大数据中心和一个本地数据服务节点：中国机房、美国西部 AWS 机房、美国东部 Azure 机房、欧洲 AWS 机房、西欧 Azure 机房和印度机房（各数据中心之间物理隔离不互通）和俄罗斯用户数据服务节点。根据用户所在地区提供相应的数据服务，后续会逐步开放更多机房。

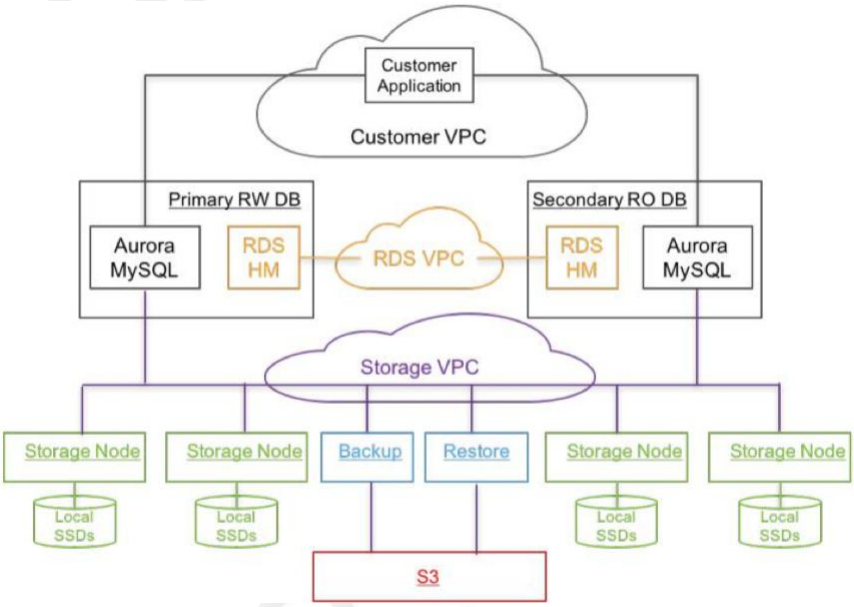
- 中国：数据保存在中国上海机房，由腾讯云提供基础云计算支持。
- 美国：美国分为西部和东部机房，西部机房位于美国俄勒冈机房，由 Amazon AWS 提供基础云计算支持，东部机房位于美国弗吉尼亚北部，由 Microsoft Azure 提供基础云计算支持。默认服务和数据默认存储在美西 AWS 机房，客户可选其服务是否使用美东 Azure 机房。
- 欧盟国家：欧洲有两个机房，其中德国法兰克福机房，由 Amazon AWS 提供基础云计算支持。西欧荷兰阿姆斯特丹 Azure 机房。默认服务和数据存储在德国法兰克福，客户可选其服务是否使用西欧 Azure 机房。
- 印度：数据保存在孟买机房，由 Amazon AWS 提供基础云计算支持。
- 俄罗斯：为了应对俄罗斯用户隐私数据本地化的需求，俄罗斯单独设立用户数据服务存储节点，由腾讯云提供基础云计算支持。
- 其它国家：根据就近原则选择(俄勒冈或法兰克福)机房存储，后续会逐步开放更多

区域机房，目前多个地区的机房在建设中。

- 数据多副本冗余存储

采用分布式架构，所有业务服务器同时部署于同城不同区域的三个机房，数据库等数据存储服务采用多副本模式(最少保证二个实时副本)，并实时进行数据备份。从物理层面保障了数据和服务的高可靠性和高可用性。

涂鸦数据库均使用云数据库，默认主从复制模式，主库和从库分布在不同的可用区。磁盘全部使用本地 SSD 硬盘，支持磁盘的自动扩展。数据的全量和增量备份全部保存在云存储上。



数据备份和跨机房同步，会进行严格的数据完整性校验，保障同步或备份数据的完整性。

3） 数据安全处理

- 数据分类分级

参照《涂鸦信息分类分级和处理策略》区分个人数据、平台信息数据和企业内部数据，根据不同的数据类型实行相应的安全要求和对策。

- 数据访问控制措施

➢ 涂鸦云采取精细粒度的云数据和存储访问权限控制。包括对应用的统一权限管控，和根据用户类型分配最小，仅必要的权限。

➢ 对于重要或敏感数据的操作执行内部审批流程。

➢ 对安全管理人员、数据操作人员、审计人员的角色进行分离设置。

- 数据过滤

涂鸦云对所有服务入口的数据进行类型、长度、格式等强制严格校验，保证数据的完整性和不被污染。

- 数据审计

完备的数据使用记录，包括对应用或用户的审计。对于高危的数据处理，需要对应的合规审计员进行审批，才能执行。

- 数据展示

原则上不得展示原始数据，因此涂鸦去标识化或脱敏处理等措施展示个人敏感数据，特殊的业务场景需要明确的隐私数据，或者响应客户的数据展示需求，通过鼠标滑动或点击显示等方式防止直接显示用户数据，以降低个人信息在展示环节的泄露风险。

- 个人数据去标志化处理

收集个人数据后，涂鸦会进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的数据分开存储，并确保在后续的个人数据处理中不重新识别

个人。

4） 数据保留策略

个人信息保存期限为实现目的所必需的最短时间，超出保存期限，应客户要求涂鸦会对用户数据删除或匿名化处理，并将数据安全返还给客户，因此涂鸦采取了【数据保留期限最小化】的原则：

- 用户个人数据的保留仅限在用户表示了明确同意，使其个人数据应用于服务相关的目的，且不得用于未经用户同意的其他任何额外用途，公司内部统一收集和维护这些数据应被保留的时效信息。
- 依法需要被保留的数据，或公司有能力证明为业务目的而必需的数据，可以在明确的数据保留时间表指定的时间内进行保留。
- 用于实现客户或第三方的正当利益而保留的数据，只能在公司与客户或第三方有明确合同约定或指示的情况下进行保留，例如为客户提供服务或其他目的提供服务时。
- 依据【数据保留期限最小化】原则，客户有权决定数据保留策略并及时告知涂鸦用于服务目的等。当客户要求删除数据或者返还数据时，涂鸦将按照此明确指示进行执行。

残留数据清除

- 曾经存储过客户数据的内存和磁盘，一旦释放和回收，其所有信息将被自动进行零值覆盖。同时，任何更换和淘汰的存储设备，都将由云服务器基础设施提供方统一执行消磁处理并物理销毁之后，才能运出数据中心。

5.3.4 数据安全和隐私保护的技术保障

1） 数据安全传输

- 数据传输完整性

应用程序处理数据传输过程，都会进行完整性校验，通常使用 HMAC—SHA256 算法。

- 内容脱敏或加密

涂鸦方案的 APP 和云之间的通讯，设备和云之间的通讯，APP 和设备之间的通讯，设备和设备之间的通讯。都采用了 AES—128 对通讯内容进行加密，特殊的内容，包括密码、生物特征数据等都进行不可逆的摘要算法脱敏后传输。

- 传输通道加密

涂鸦方案的 APP 和云之间的通讯，设备和云之间的通讯，不管是 HTTP 或 MQTT 都使用 TLS1.2 协议进行通讯，并且执行严格的证书校验。

2） 设备端数据安全

涂鸦云提供多重安全策略保障智能设备产生的数据安全性。如下图：

- 设备与云端通讯保护
  - 数据加密：使用 AES128 加密数据内容。
  - 身份识别：涂鸦自有算法保障设备连接认证，请求授权，指令下发等多重交互认证、访问控制和有效授权的保障。
  - 动态密钥：一机双码，包括动态密钥和动态口令，保障设备安全。
  - 通道加密：全链路 TLS1.2 数据加密传输协议，且双向强制认证。
  - 安全芯片：部分芯片支持选择使用带安全芯片版本，用来安全存储硬件授权信息和加密 key 等。
  - 虚拟设备设计：保证了设备授权信息被盗取后，不影响原有设备的正常使用，同时使用设备匿名化技术保障用户隐私安全。
- 设备局域网通讯保护

- 数据加密：使用 AES128 加密数据内容，在局域网内传输。
- 动态密钥：配网时算法动态分配。

云平台安全保障，详见第 7 章。

设备端安全保护，详见第 10 章。

5.3.5 数据保护的组织安全

1) 数据跨境传输

随着国际环境对于数据安全和隐私保护多变要求，涂鸦实时关注对于数据跨境传输的国际动态。比如欧盟出具的标准数据跨境协议保证了欧盟区域向其他区域数据传输的法律基础，涂鸦也关注其他区域/国家/地区对于数据传输的法律合规基础，并及时作出响应。

总体而言，涂鸦严格遵循“数据本地化要求”和“非必要不同步”的大原则下，用户个人数据最大程度存储在本地服务器，不同步到其他区域。

鉴于涂鸦业务管理和经营需要，涂鸦有权限处理各个数据中心的数据，此类型的数据处理也构成了数据跨境传输，但对于此类远程访问数据的形式，数据保护法律法规完全认可，符合数据跨境传输法规；

2) 数据安全处理权限管控

根据“数据处理权限最小化”原则，涂鸦严格管理对客户个人数据享有权限的人员，明确职责分工，规范数据处理流程，定期审核权限，并加强数据安全培训。

5.3.6 数据共享

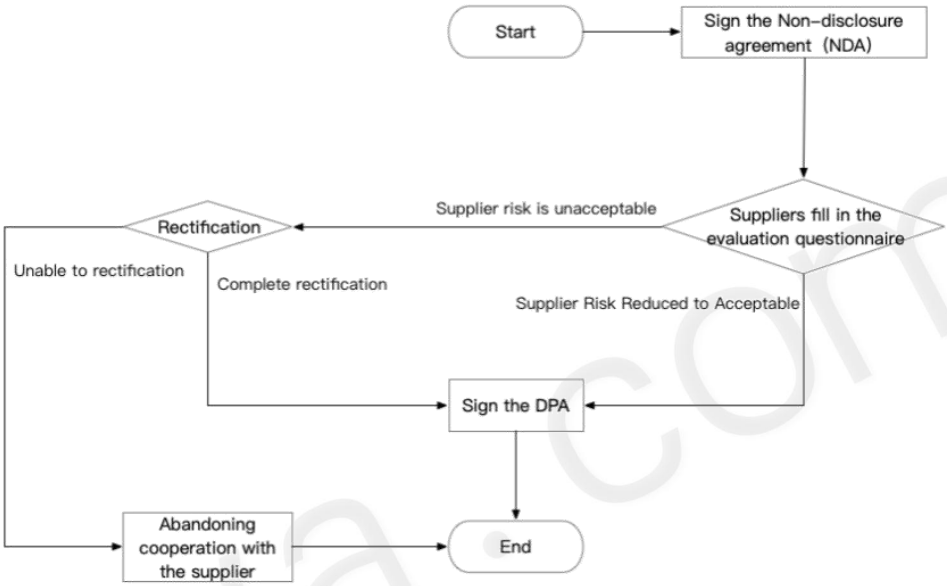
涂鸦根据各种服务场景的需要，并在合法合理的前提下，与三方服务提供商或合作伙伴进行数据共享，主要有：

- 第三方智能场景入口服务商，比如 Google、AWS，需要用户主动授权其账号数据共享给到对应的语音平台，从而实现类似 Google Home，AWS Echo 等对涂鸦平台用户智能家居场景的支持。
- 第三方软件服务供应商以支持特定服务，比如短信和电话服务提供商 Nexmo，手机消息推送 Google 或 Apple 服务，涂鸦恪守最小化数据原则对该部分服务所需数据进行共享。如涉及隐私数据的共享，涂鸦对此三方供应商和合作伙伴进行严格的供应商审核，包括对隐私安全合规的审计。

对于用户个人信息原则上禁止共享。如特殊原因需要共享，需对供应商进行完善的隐私风险影响评估。同时需要向个人信息主体告知共享个人信息的目的，数据接收方的类型，并事先征得个人信息主体的授权同意。

5.4 供应商安全隐私审核

在涂鸦提供完备的针对性服务中，涂鸦授权可信赖的第三方数据处理机构进行必要的数据处理活动。涂鸦遵照《供应商审核流程》进行数据安全及隐私保护方面严格审核，审核根据产品或者项目特性，一般包含 GDPR 评估、PIA/DPIA 评估，其评估流程，如下：



其中，借助隐私合规评估工具，我们首先采用合格版本的安全和隐私合规问卷，对供应商进行标准化评估，当供应商存有不可容忍的不符合点，涂鸦将强制性要求其整改，否则不得进入供应商服务名单。

对供应商安全能力评估包括安全开发生命周期管理流程、漏洞管理流程、数据安全生命周期管理流程、权限控制、服务与数据灾备、人员与组织安全管理、渗透测试规范和支撑、合规认证、密钥管理、网络安全防护体系和设施、安全事件响应机制、变更管理等。

6. 安全组织和人员

为了提升涂鸦所有员工信息安全意识，更好地保障客户利益和产品与服务信誉，涂鸦在公司内部倡导“人人懂安全”的理念和实践，创造了一个无时不在，无处不在，充满活力和竞争力的安全文化。这种文化的影响贯穿在涂鸦招聘选才、员工入职、上岗培训、持续培训、内部调动和离职等各个环节。每位涂鸦的员工都积极参与建立并保持涂鸦产品和服务的安全，并按的规定实施各项安全活动。

6.1 安全与隐私保护团队和人员

涂鸦有专业和完整的安全技术团队，该团队成员曾就职于阿里、蚂蚁金服、百度等互联网公司和传统安全厂商绿盟科技、启明星辰、安恒等，支持涂鸦云的安全质量保障、安全评估和安全运维工作。同时该团队在隐私安全合规层面，有来自美国道富银行等的专业人才和外聘的专业隐私安全合作机构，以及专注于网络安全和隐私保护全球性、地域性律师事务所提供专业咨询服务。确保公司安全和合规体系架构上在每个层次、每个环节都做到可控、可信、可靠。

6.2 安全合规委员会

同时，涂鸦内部成立了安全合规委员会，由关键创始人带领委员会，包括 CEO、CTO、CFO 等高级管里层共同承诺对信息安全与隐私合规的支持，信息安全统一目标的制定，并以遵守法规和合规性要求为基线，为涂鸦（包括运营和业务利益相关方）提供风险和合规性支持。

安全合规委员会每个季度执行一次正式会议，讨论对安全合规目标实现的汇总和下阶段主要目标的确认，并对合规工作的开展提供支持。

6.3 人员安全管理

涂鸦的人力资源管理框架和公司的整体人力资源管理框架一致，都是建立在法律基础之上。于此同时，《人力资源基本制度》对于员工从招聘，员工合同制度化管理，涉及信息安全的考勤管理，离职程序化管理等方面规范流程以加强人员安全管理。

HR 会在发放 Offer 前，对候选人执行严格的背景调查来保障员工背景和资历适合涂鸦业务的需要。员工行为符合所有法律、政策、流程以及涂鸦商业行为准则的要求。员工有履行其职责必备的知识、技能和经验。

涂鸦在员工入职需要签署的雇佣协议遵守规定的信息治理和安全政策的规定和条款。同时，还需要签署保密协议。保密协议严格约束了具体明确的保密范围，保护包括涂鸦、涂鸦员工和涂鸦客户在内的机密和敏感数据，包括商业机密、技术机密、员工信息和客户或用户的隐私数据等。只有完成这些协议的签署，才允许使用或接触公司的资产。

员工离职，会有严格的自动化和人工审批流程，包括工作交接的要求和离职前对于其电子设备、服务器、各种账号等资源和资产的回收。高职级和特殊的岗位，还需要进行员工合规的审计，包括对其离职前的一些办公行为进行审计。

6.4 安全意识教育与纪律约束

为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，涂鸦内部发布了《涂鸦智能员工信息安全手册》，并以此为基准定期开展网络安全意识教育学习，要求员工持续学习网络安全知识，了解手册实质性内容。知道哪些行为是可以接受，哪些是不能接受的，意识到即使主观上没有恶意，也要对自己的行为负责，并承诺按要求执行。

涂鸦《员工信息安全手册》与员工安全意识和行为进行佐证，进行每个季度的考核和教育，对员工日常办公等安全纪律进行规范。对于严格遵照信息安全手册以及安全规范落实到位的团队，公司将公开表彰；而针对违反安全政策和程序的员工制定了正式的惩罚措施，以引起全员重视。

6.5 安全管理体系相关培训

为了让公司全员能够准确理解公司信息安全管理政策，并且有效推动和落实安全策略，每个季度涂鸦安全团队和内审团队进行隐私保护合规和数据保护相关的培训。并有严格的考核通过要求。未通过的员工需要持续学习直到通过考核。

信息安全培训通过线上线下方式呈现，包括但不限于安全开发培训，渗透测试培训，漏洞培训，安全架构培训，合规体系培训，安全开发流程培训等。

6.6 信息安全能力提升

涂鸦内部会定期的举行安全开发培训和信息安全交流，旨在提升员工的安全技能，确保员工有能力交付安全、合规的产品、解决方案和服务。

7. 云平台安全保障

7.1 物理安全

涂鸦作为物联网云计算服务提供商，涂鸦云平台着力为每一个客户提供安全、稳定、持续、可靠的物理设施基础。涂鸦云依据数据中心相关的国际标准和监管要求，建立了一套全方位的安全管理体系，从制度策略，到流程管理，并配合严格的监察审计，通过持续改进来保证云平台数据中心的物理和环境安全。

7.1.1 高可用的基础设施

涂鸦云平台整合全球最知名的云主机服务商 AWS、Azure 和腾讯云等，构建全球服务节点。为客户提供安全、稳定、持续、可靠的物理设施基础。

1320+	6	8	1
CDN Acceleration Nodes	Global Regional Data Center	Media Acceleration Node	Local Data Service Node

涂鸦云根据中国企业内外销区域结合海底光缆分布和全球各城市的实测结果，部署覆盖中国、欧洲西部、欧洲东部、美国西部、美国东部和印度六个可用区和一个俄罗斯本地数据服务节点。

包含但不限于美国西部俄勒冈 AWS 数据中心、美国东部弗吉尼亚 Azure 数据中心、欧洲法兰克福 AWS 数据中心、欧洲阿姆斯特丹 Azure 数据中心、腾讯云上海机房和腾讯云俄罗斯莫斯科本地服务节点等，其他机房包括香港、新加坡、孟买、东京、圣保罗多个机房等（可根据企业客户所在区域动态扩容可用区）。

涂鸦云灵活地将数据和系统部署于不同数据中心或不同区域，以保证业务的容灾性要求。

7.1.2 安全检查和审计

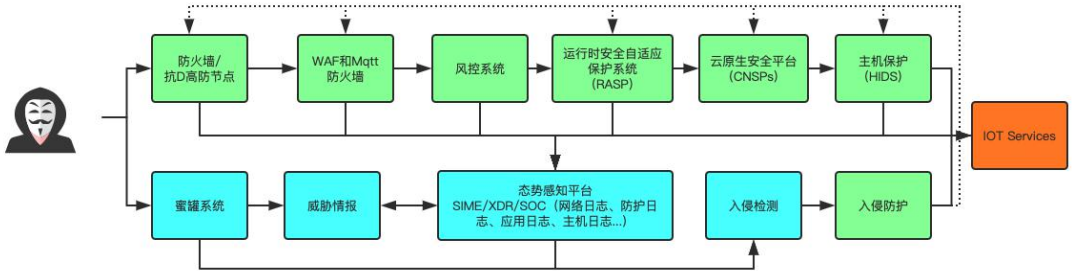
安全事件管理：和云服务器供应平台达成物理安全应急预案，并定期组织数据中心工作人员进行安全演练。一旦发生物理安全事件，该预案将能够立即生效并指导相关人员以最大可能保护客户资产。

7.2 网络安全

7.2.1 安全架构

涂鸦云拥有成熟的网络安全架构，包含防火墙、WEB 应用防火墙、MQTT 应用防火墙、入侵检测、RASP、主机防护系统、抗 D 系统、云原生安全平台、SIME 等多重防护机制，以应对来自互联网的各种威胁。

涂鸦云的网络防护架构图如下：



7.2.2 网络通信安全

涂鸦云平台上的通信均采用 TLS1.2 安全协议，包括设备和 APP 与云端的通讯，并且提供的 API 接口也具有完善的 TLS 等安全能力，能够对客户提供端口级别的安全保障。同时，通讯的内容额外使用 AES128 加密，密钥基于每个设备和用户随机生成，保证了密钥的唯一性和安全性。双层加密保护通讯过程的安全。

7.2.3 网络隔离和访问控制

涂鸦制定了严格的内部网络隔离规则。通过物理和逻辑隔离方式实现内部的办公网络、开发网络、测试网络、生产网络等的访问控制和边界防护。涂鸦云确保非授权人员禁止访问任何内部网络资源。所有员工如需从公司网络前往生产网络开展日常运维时，都必须经过堡垒机的严格审批和权限控制，才能使用受限的权限登录生产系统，并且使用全程有审计。

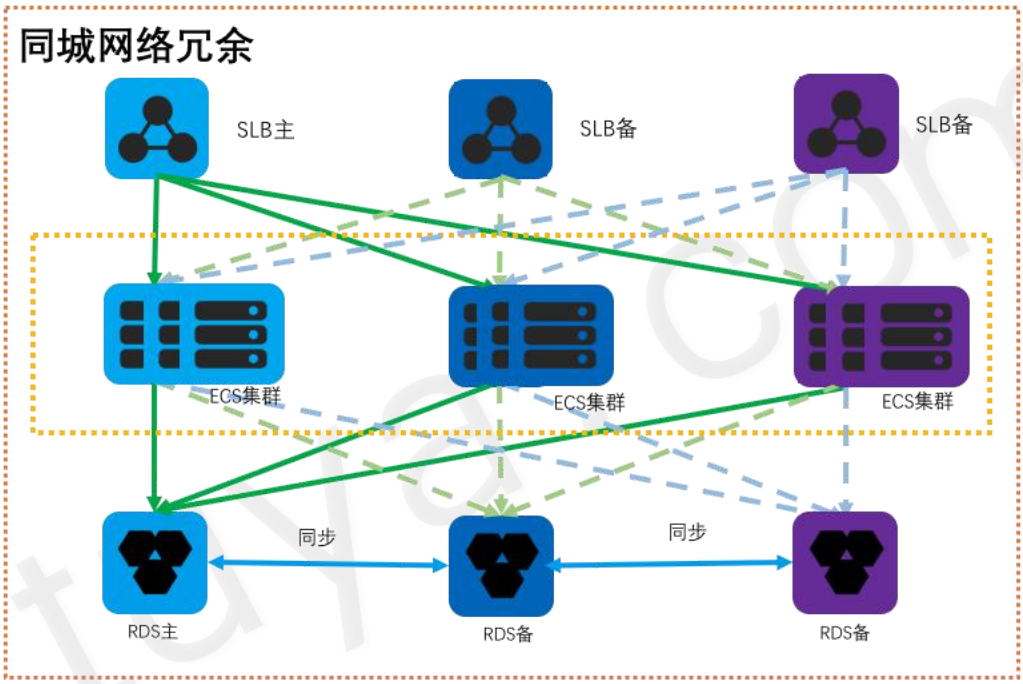
针对云端用户层面的网络访问隔离，涂鸦提供虚拟化控制层资源访问控制策略、云平台内部私有网络间隔离策略、WEB 控制台权限分配与身份验证、接口会话 ID 与访问密钥等安全机制，确保客户只能访问其用户产生的相关数据，有效实现多客户之间的访问隔离。

7.2.4 网络冗余

涂鸦云数据服务云主机遍布全球多个区域，构建了网络跨地域的灾备能力，能够最大化的减小非人为因素导致的网络故障的业务影响。

同时，采用冗余的网络建设方式，同时同城也采用多物理机房部署，能够实现网络的便捷性和流量附和的工程调度，确保网络服务不会因为单点故障而中断，实现同城和跨城容灾。

同城多机房网络冗余部署如下图：



7.2.5 DDoS 防护

涂鸦云自建抗 DDoS 高仿集群，能够对一定流量的 DDoS 攻击进行拦截，包括对网络层的

IP 地址扫描、畸形报文攻击和分片攻击进行拦截；能够对传输层常见的 TCP Flood、UDP Flood、发射放大攻击、TCP/UDP 分片报文攻击、畸形报文攻击、DNS 投毒等进行识别和拦截；能够对应用层 CC 攻击、HTTP 慢速攻击、SSL DDoS 攻击、SIP Flood 和 MQTT 连接攻击进行识别和拦截。

同时，涂鸦为了保障业务的稳定性，同时开启了 AWS、微软 Azure 等云平台的 DDoS 防护功能保护所有数据中心，自动检测、调度和清洗能力。

对于 CC 攻击(Challenge Collapsar)，内部通过防火墙和 WAF 也进行了一定程度的异常连接的限制和阻断。同时内部通过对所有请求日志的分析和结合第三方威胁情报数据，进行异常的 IP 进行检测，动态屏蔽可疑的源地址。

7.3 入侵防护

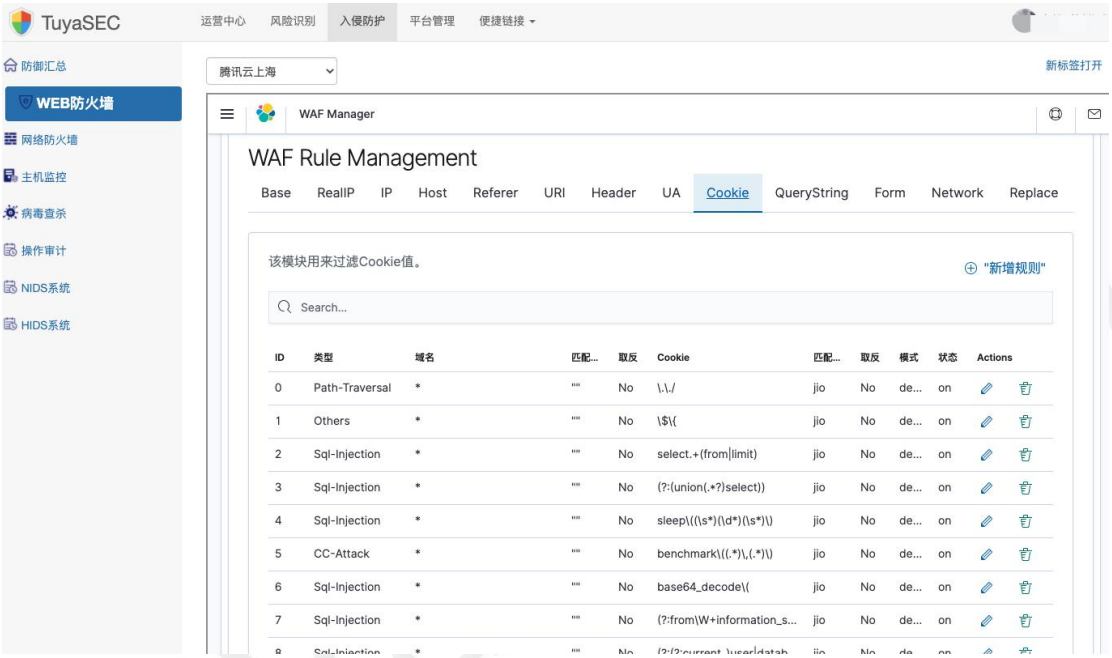
7.3.1 网络入侵检测

通过对所有服务器，应用、网络等进行实时的日志审计和安全分析，能够快速发现安全风险，告知安全团队。通过会调用第三方威胁情报接口，如果涉及异常的 IP 地址、域名地址等威胁情报信息，则自动化进行防火墙和 WAF 的阻断。

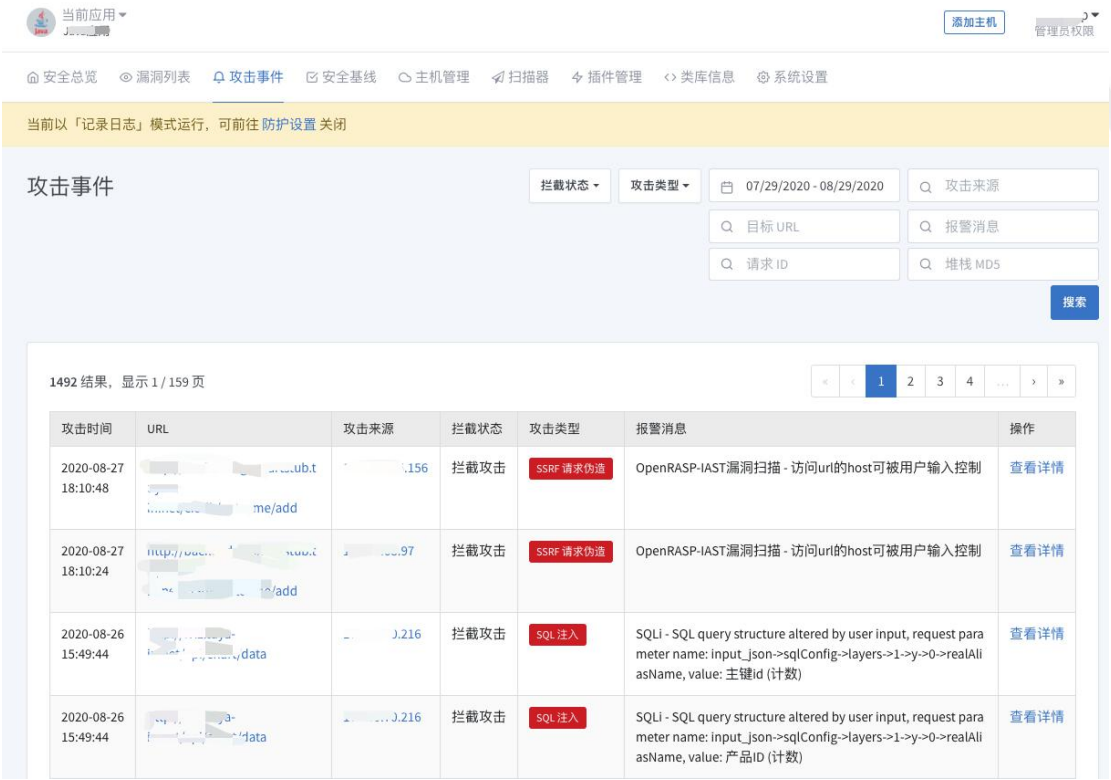
7.3.2 网络入侵防护

通过网络防火墙、WEB 应用防火墙（WAF）、MQTT 应用防火墙（EWAF）、RASP 和云原生安全平台等安全防护工具进行入侵阻断。

WAF 和 EWAF 能够实现对应用请求数据流的分析，通过规则进行匹配和拦截。

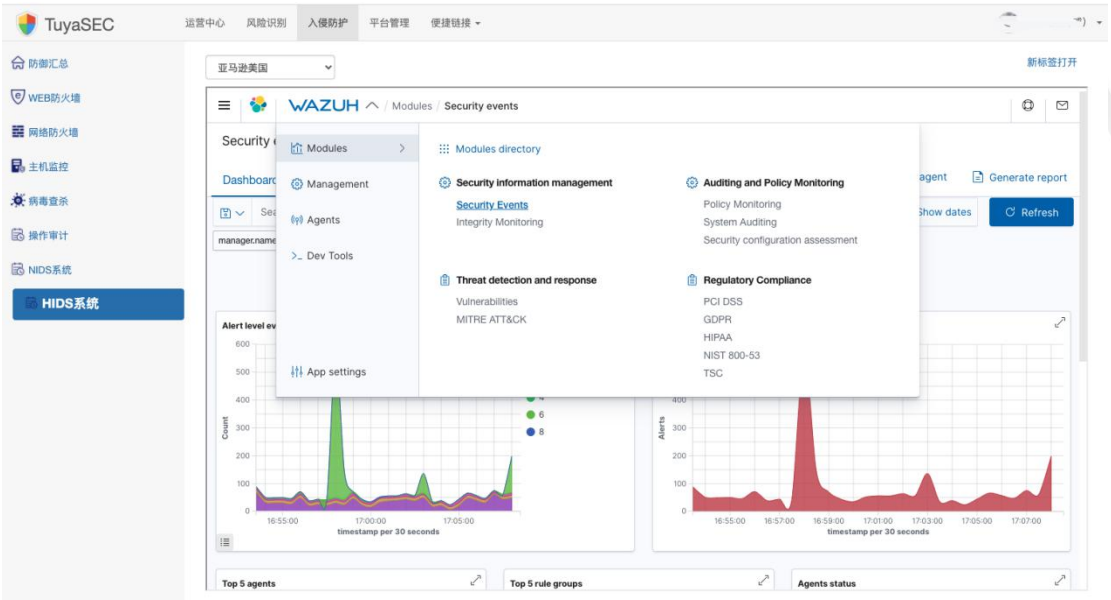


RASP（应用运行时自我保护）能够直接注入到被保护应用的服务中提供函数级别的实时防护，可以在不更新策略以及不升级被保护应用代码的情况下检测和防护未知漏洞。



7.3.3 主机安全检测

包括 WebShell 检测模块，服务器部署了 WebShell 实时检测引擎，能够实时检测、删除和上报 WebShell。主机异常登录检测模块，能够识别机器被非堡垒机登录。不安全基线配置检测模块，能够识别机器是否按照安全基线配置上线。主机漏洞检测模块，能够识别主机的应用漏洞和系统漏洞。还有系统状态异常模块、配置文件变更告警模块等。



7.3.4 数据库审计

涂鸦有数据库管理平台（DMS）对数据库的权限进行严格的统一管理和限制，并且对所有数据库的增删改查都进行完备的日志审计。

7.3.5 病毒查杀

触发式检查所有业务接口上传的文件。同时，也保持定期检查文件存储服务器的文件安全，是否存在病毒，或可执行文件等。

7.4. 业务安全与风控

7.4.1 账号安全

账号安全是涂鸦云服务体系的基础，所以针对账号的注册、登录、密码找回、多设备登录等都进行了严格的安全管控和日志审计。同时，针对账号体系的数据存储、查询和修改都进行了严格的保护。针对撞库、API 滥用等常见账号风险来源进行严格的策略保护。

目前在所有登录、重置密码等登录相关的接口，全都使用无痕或滑动式的验证码，保障了业务人机识别的能力，防止恶意注册、撞库等攻击行为。

同时，对用户注册时候，弱密码的检查，禁止常见弱密码的设置。

7.4.2 设备认证

涂鸦模组在生产的时候，会写入一对设备认证信息，这些信息在所有设备中都是唯一的，与模组的环境绑定，包括芯片 ID 和 MAC 地址等，在每个会话请求中，签名数据包的时候加签了这些信息。每个通讯都必须保证模组的环境信息和设备认证信息准确，才能够有效通讯。

7.4.3 内容安全

涂鸦在所有文件上传入口都进行了统一的业务文件类型识别和病毒扫描、木马扫描引擎，能够快速识别上传的文件的安全风险。

7.4.4 密钥管理

涂鸦拥有安全可靠的密钥管理体系和完整的密钥全生命周期的管理，包括创建、激活、禁用、转换、分发、备份、销毁等。同时基于密钥的数据加密存储。

在智能设备端，初始的密钥信息是生产写入设备安全区，在设备完成认证和用户绑定后，生成随机密钥。同时使用在设备本地数据加密的密钥是通过设备信息随机生成，仅在本地有效。

在云端有统一的密钥管理系统 KMS 服务，用来支持密钥的创建和管理，能够有效保护密钥的保密性、完整性和可用性，同时有完善的审计功能，满足了监管和合规的要求。

7.4.5 证书管理

对于服务器、终端的设备证书等，涂鸦自研发了一套证书管理系统，配套证书调用的 Client，通过 client 实现代码部署 0 接触证书，即可实现可信调用和配置。同时该证书管理系统对证书等信息进行加密存储。提供业务支持基于域名、终端信息、固件信息等证书的签发、验签等功能。

7.4.6 配置管理

涂鸦内部不允许任何硬编码重要配置，包括秘钥、证书、数据库配置等信息。所有配置需要通过应用认证后接入配置中心拉取到对应的配置。该配置中心接入证书管理和密钥管理系统，实现统一的配置管理。同时对于每个应用的认证和权限管理，都需要经过特定的审批流程，才允许业务调用。

8. 安全开发周期管理（SDLC）

涂鸦严格按照安全开发生命周期方法开发云、APP 和智能设备三端服务和产品，目标是将

信息安全融入到整个软件开发生命周期中。

涂鸦的开发生命安全周期，全面涵盖了系统开发生命周期的各个阶段。

通过安全管理平台进行统一的项目 SDLC 实施监控和管理，基本实现全自动化的流程跟踪和自动化安全评级。

8.1 安全需求分析和产品设计

需求分析阶段，涂鸦安全团队会根据功能需求文档进行安全需求分析，针对业务内容、业务流程、技术框架进行沟通，提出安全需求，并与业务方、开发人员就其中建议达成共识。

产品设计阶段，涂鸦安全团队对系统进行攻击面分析、威胁建模和隐私风险评估，对产品设计中采用的技术进行安全评估，使用到的数据进行隐私合规评估，提出安全和隐私风险，并与开发人员就安全建议达成共识以解决认定风险。

8.2 开发阶段

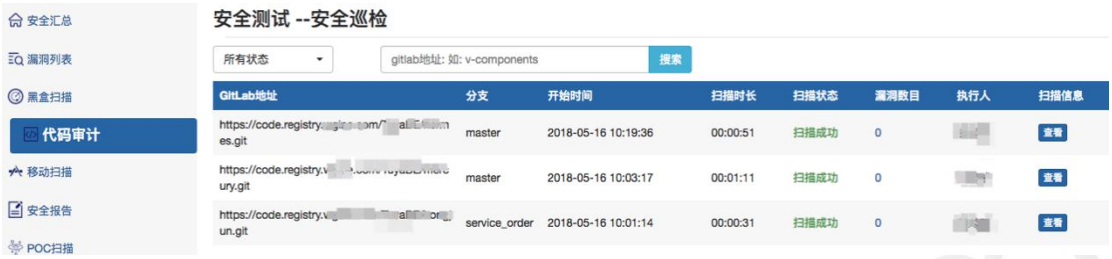
8.2.1 安全开发规范

开发编码阶段，涂鸦安全团队设计了安全的开发框架供开发人员使用，同时要求开发人员严格遵循安全编码规范，并提供自动化的安全 IDE 插件，对开发人员在编码中出现的安全风险进行提醒。同时每完成一次代码提交，都会进行自动化的代码审计，并通知对应开发进行安全修复。

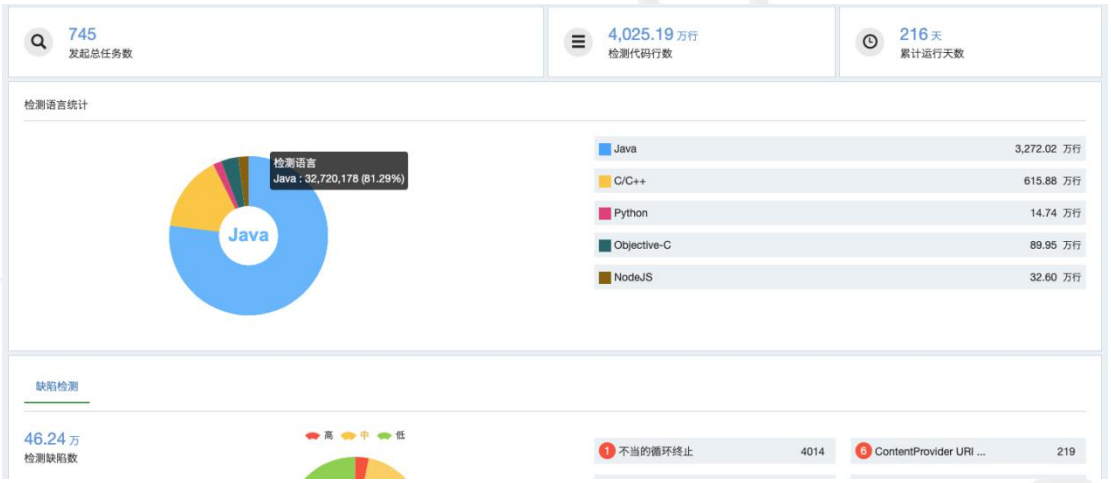
涂鸦安全编码规范遵循国际主流的编码规范，包括美国国家标准和技术协会 NIST 的相关标准、欧洲电信标准协会 ETSI 的相关标准、OWASP 的相关标准。

8.2.2 代码审计

涂鸦自主开发的代码审计，绑定了涂鸦的项目发布系统，项目到预发阶段，自动化进行代码审计测试。该工具通过语法树分析，能够准确找到高危的风险函数入口，并对函数的使用前进回溯分析，找到不安全的使用。



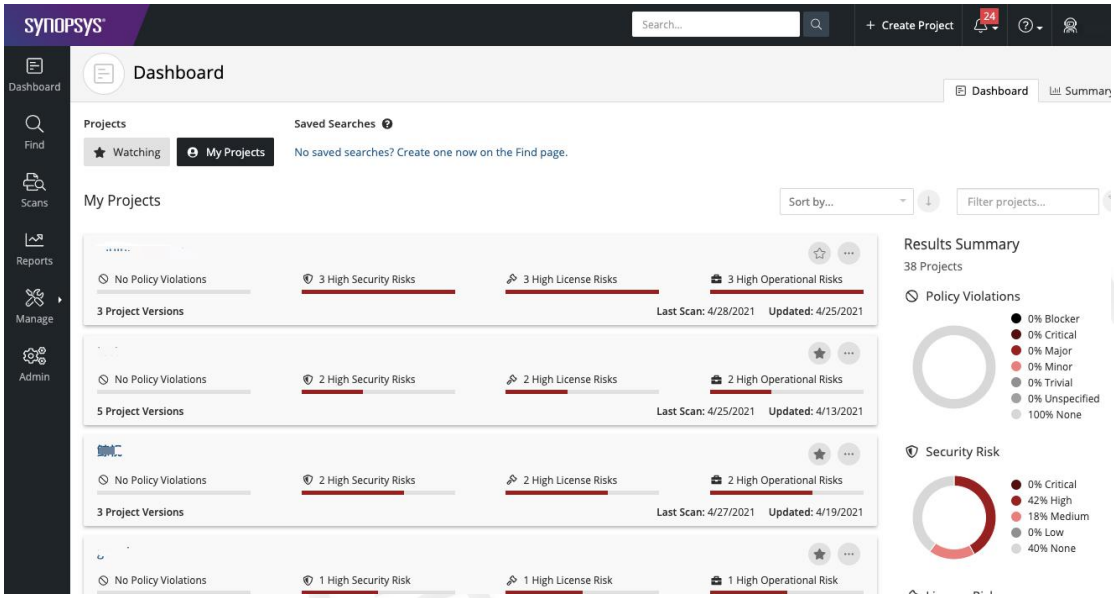
同时涂鸦还集成了国际主流的第三方代码审计工具，通过该工具实现对涂鸦主要语言的支持，能够有效帮助到业务进行漏洞发现。



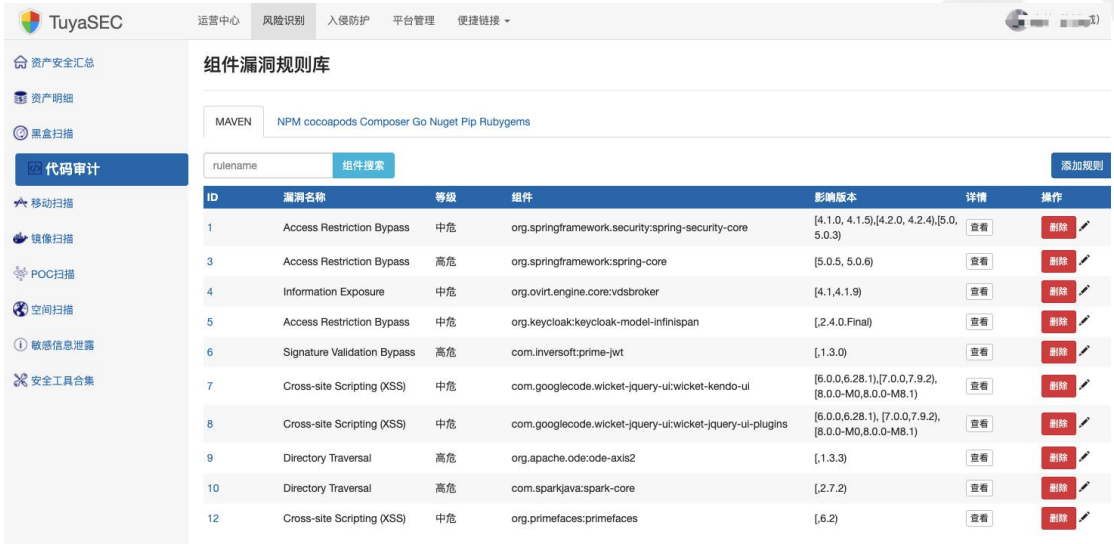
8.2.3 开源审计

涂鸦安全团队部署了国际上开源审计最佳解决方案 blackduck，并接入了多端 CICD 进行代码发布前和第三方 SDK 或二进制固件包的安全检测。

Blackduck 能够识别和追踪应用程序和容器的开源组件，能够发现和协助开发修复开源漏洞，能够验证和遵从开源许可证的条款。通过 blackduck 的产品和期背后专业的安全洞察团队，能够保障内部业务能够第一时间发现开源组建或供应链的安全问题。



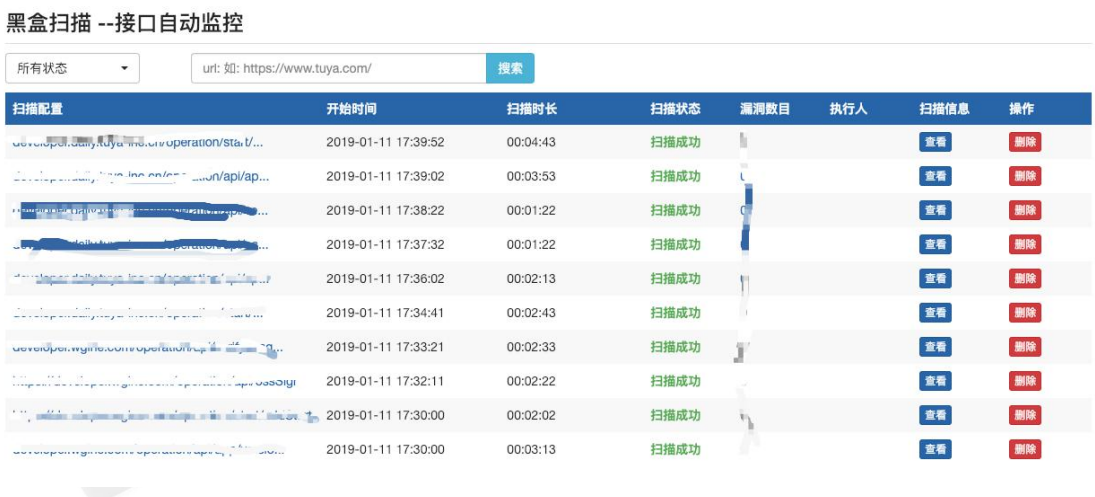
除了使用 blackduck 的方案，涂鸦还自研代码开源扫描器，作为一定的补充。涂鸦自研的扫描器也同时接入了涂鸦发布流程的自动化审计，能够识别代码中引入的所有组件，通过和风险组件规则库进行匹配，分析不安全的组件，形成自动化组件漏洞生成并推送给到具体的开发进行漏洞修复。同时其漏洞库实时从主流漏洞披露网站上更新。



对于源代码的使用和管理，涂鸦有严格规范，通过 blackduck 对功能的评估、流行程度、开发社区活跃度、文档完善度和许可证评估进行综合的矩阵判断。同时，进行必要的使用审批、测试和安全审计。特别地，涂鸦对许可证的合规有严格的风险定义，禁止引入合规风险。

8.2.4 黑盒扫描

针对业务接口，涂鸦采用被动扫描代理服务器，只要接入代理，进行测试，黑盒扫描器能够自动捕获项目接口进行自动化的安全审计。



8.2.5 移动扫描

涂鸦 APP 打包平台，在完成新 APP 打包后，会自动发送 APP 包到移动扫描平台进行扫描，

支持安卓和 IOS 的 APP。

8.2.6 灰盒扫描（IAST）

IAST（交互式扫描）技术是一种实时动态交互的漏洞检测技术，通过结合涂鸦服务中所有 RASP 节点客户端，收集、监控 Web 应用程序运行时函数执行、数据传输，并与扫描器端进行实时交互，高效、准确的识别安全缺陷及漏洞。

8.2.7 部署环境安全扫描

针对应用的部署环境，包括端口、域名、服务器和对应的镜像，涂鸦都会进行基线安全审计和使用工具进行持续性基线安全监控，包括不安全配置、版本漏洞、合规基线等，同时联动到项目流程中，发布除了保证代码本身质量，同时也保证了部署环境的安全。

8.3 安全测试和修复验证

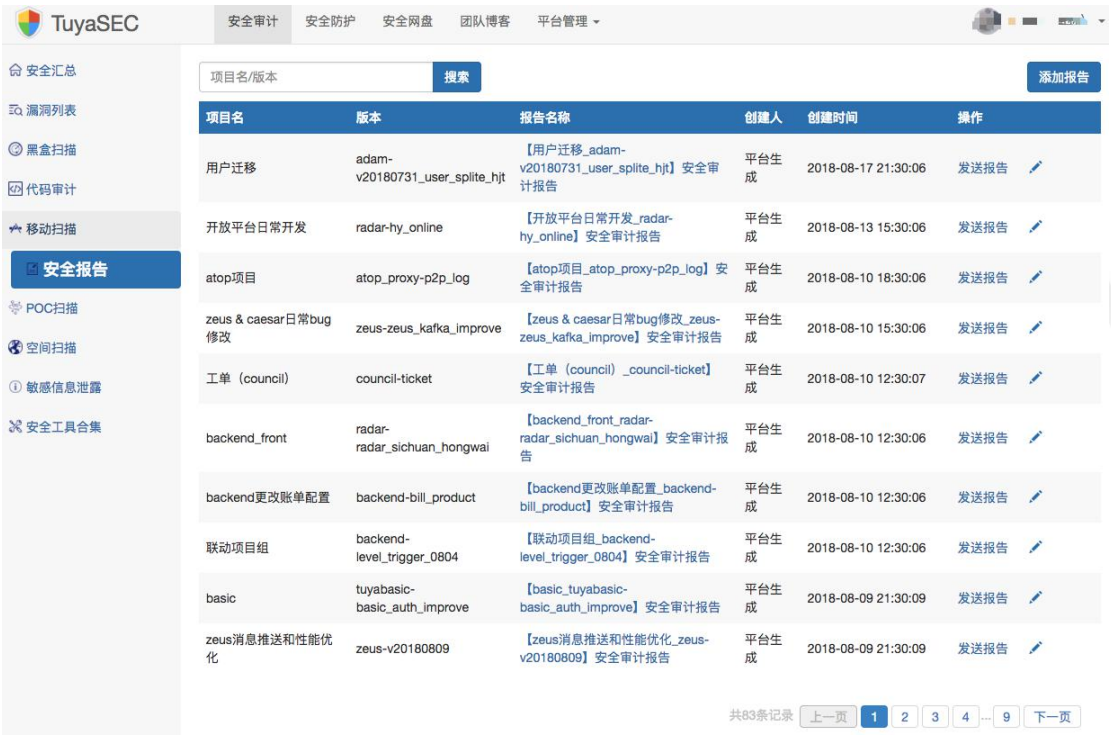
8.3.1 安全测试

测试阶段，涂鸦安全团队通过漏洞扫描平台、代码审计、移动扫描等工具并结合手工测试，进行安全渗透发现漏洞，发现漏洞后，通过工单系统对漏洞修复进行针对性的跟踪。

涂鸦渗透测试遵循行业主流的标准，参考包括 OWASP top10, OWASP mobile top10, EN 303 645, OWASP Top10 Privacy Risks Project 等。

8.3.2 漏洞修复和安全评估报告

发布阶段，只有经过安全测试，完成所有中高危漏洞的修复，得到《安全测试报告》，系统才能发布到生产环境，能够有效防止产品携带安全漏洞在生产环境运行。发布过程按照安全上线规范对系统进行整体加固。



9. 安全运维和运营

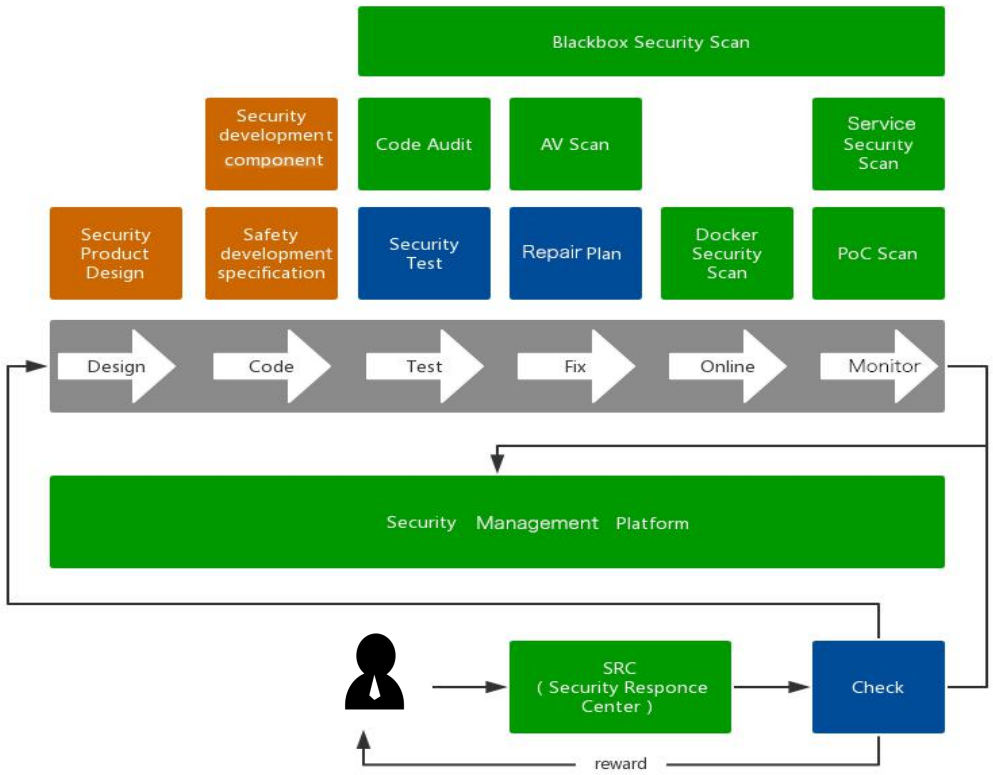
通过涂鸦的安全运维平台进行统一的管理，采取严格的访问控制、监控审计来确保运维安全。

- 账号管理和身份认证：使用统一的账号管理和身份认证系统管理员工账号生命周期，每个员工存在唯一的账号；集中下发密码策略，强制密码强度，并要求定期修改密码，同时使用多因素认证，需要安装涂鸦内部 APP，获取动态验证码进行登录二次校验。
- 授权：涂鸦基于员工工作岗位和角色，遵循最小权限和职责分离原则，授予员工有限的资源访问权限。员工根据工作需要通过集中的权限管理平台申请各种访问权限，经主管、数据或系统所有者、安全管理员以及相关部门审批后，进行授权。
- 监控：涂鸦云使用自动化监控系统对云平台网络设备、服务器、数据库、应用集群以及核心业务进行全面实时监控。监控系统广泛使用仪表盘展示涂鸦云关键运营指标，并可配置告警阈值，当关键运营指标超过设置的告警阈值时，自动通知运维和管理人员。

- 审计：对员工对生产系统的所有运维操作必须且只能通过堡垒机进行。所有操作过程完整记录和录制下来实时传输到集中日志平台。对违规事项定义审计规则，发现违规行为并通知安全人员跟进。

9.1 安全风险管理

涂鸦安全团队在漏洞管理和发现具备专职的团队，能够发现、跟踪、追查和修复安全漏洞。



涂鸦安全团队内部出了所有业务代码上线前的安全渗透测试，同时会不定期对线上在线业务进行渗透测试。

涂鸦每年还聘请了第三方安全参与公司云服务、移动客户端、硬件产品以及涂鸦整体 IT 架构的渗透测试。

涂鸦支持外部白帽子通过涂鸦 SRC（https://src.tuya.com/）或对外的邮箱等渠道提交漏洞，并对提交者提供最高单个优质高危漏洞 10 万美金的漏洞奖金。涂鸦内部会对漏洞进行验证和评估，如果确实是漏洞，会通过工单跟踪漏洞修复，直到修复完成，涂鸦会将整个过程反馈给白帽子。

漏洞评级根据《涂鸦漏洞风险评级》中根据攻击的技术要求、受影响的规模、漏洞发现和利用的难易程度、对应的业务重要程度、漏洞可能造成的危害程度进行综合评定，内部漏洞评级参考 CVSS3.1 版本。

针对云端的漏洞修复，紧急漏洞，安全团队必须 6 个小时内完成确认，开发团队在 12 个小时内修复；高危漏洞，必须在 1 天内完成确认，2 天完成修复，中危漏洞 3 天内完成确认，一周内完成修复，低危漏洞根据业务情况进行修复周期评定。如涉及 APP 和硬件，客户可参与涂鸦 SLA 等文件中的漏洞修复时间承若。

9.1.1 资产管理

基于资产及版本的安全风险风险管理。能够快速识别资产风险。

9.1.2 安全扫描

每个月执行全网安全扫描，包括 WEB 站点漏洞扫描、应用和服务漏洞扫描、主机漏洞扫描、代码组件漏洞扫描和 IAST 实时扫描等。

9.1.3 渗透测试

渗透测试是对可能的攻击场景进行实际的演示，模拟黑客尝试绕过涂鸦网络中的安全控制，并能够获取系统中的最高权限。

涂鸦每年都会进行至少一次内部的针对涂鸦的人员、组织架构和 IT 架构进行渗透测试，测试内容包括外网渗透，内网渗透，社会工程学等。

同时，保持至少一年 1 次的第三方渗透测试，该服务由国际最专业的第三方机构提供，目前合作的机构包括 NCC Group、Kaspersky Lab、VTrust 等。由第三方机构对涂鸦的云平台、APP 和硬件产品进行全方位的安全评估和渗透测试。

此外，涂鸦通过 SRC 对外发布漏洞悬赏，还接入了第三方众测平台，旨在让全球白帽子能够由渠道报告涂鸦产品和服务的安全问题。

9.1.4 安全事件响应

涂鸦内部执行严格的安全事件和漏洞分级，针对事件的响应根据分级进行对应的处理执行程序，包括事件的报告渠道、响应、调查和纠正措施。

在影响到客户的业务稳定性和安全性时，涂鸦也会提供调查报告给客户。

9.1.5 安全风险评估

为了在考虑控制成本与风险平衡的前提下选择合适的控制目标和控制方式，将信息安全风险控制在可接受的水平，涂鸦每年至少进行一次风险评估。

安全风险评估策略，始终与涂鸦整体安全控制策略、程序及国际主流标准保持相关性和有效性。

评估过程是针对涂鸦现有服务，建立全局性的建模视图，分析系统自身内部机制中存在的危险性因素，同时又可以发现系统与外界环境交互中的不正常和有害的行为，从而完成系统脆弱点和安全威胁的定性分析，从而达到消减和控制风险的目的。

9.1.6 安全审计

涂鸦安全团队对所有安全体系的平台、工具的访问、配置变更、权限授予等过程都会进行严格的审计，并保留所有审计记录。

同时内部搭建了一套安全审计平台，对接了内部主要的管理系统，能够对所有员工访问和操作等日志进行统一审计，并且保障了审计日志的准确性、完整性和不可抵赖性。

9.2 员工权限和访问控制

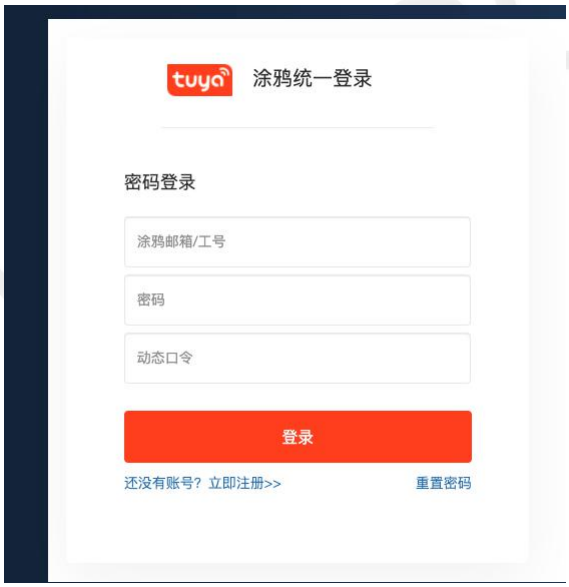
涂鸦对 IT 体系的系统权限、机器权限、数据权限等权限实现了权限统一管理，实现了零信任的权限管理模型，基于用户身份、应用身份和应用功能等的识别，实现最小化的权限控制。

9.2.1 内部系统权限管理（AAA）

其中系统权限主要包括内部系统平台权限、应用权限、机器权限等。系统权限的授权遵循“最小特权原则”，即给各权限角色分配且仅分配其完成任务或操作所需的“必不可少”的权限。

同时系统严格记录所有权限更变的审计记录等。

针对内部系统的身份认证，涂鸦对内部所有应用实施了单点登录技术（SSO），同时，SSO 实现了 OTP 的能力，除了满足目前所有合规的密码管理要求，同时还增加了每次登陆动态码校验的能力。

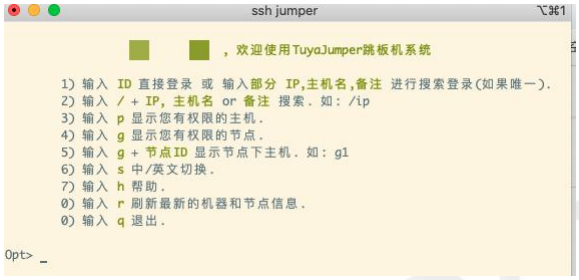


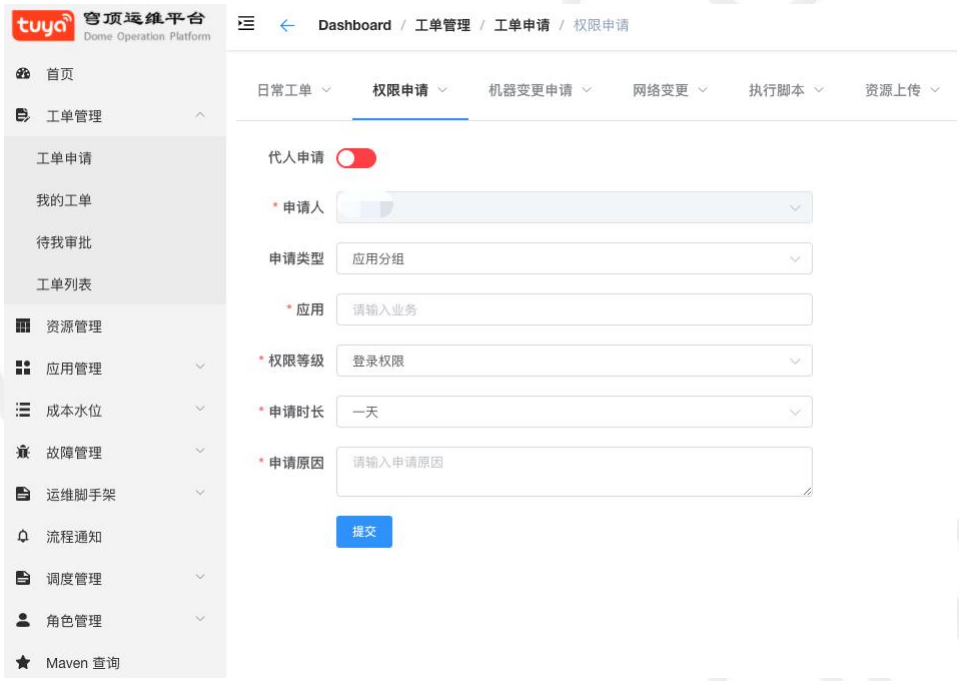
针对内部系统的权限校验，涂鸦有统一的权限管理系统（ACL），该系统实现了对应用、应用功能、数据的授权。平台上有完善的审批流程管理等。

9.2.2 机器权限管理

涂鸦员工对机器的权限申请和审批有统一的管理平台。需要对应的主管、运维、安全和应用负责人进行审批，才能完成权限的下发。员工被授权后通过登录堡垒机实现对机器有限权限

的控制。同时，权限审批流程、机器登录会话、命令、文件传输等拥有完整的审计流程。





9.2.3 应用权限管理

涂鸦对每个应用，应用与应用之间的调用等权限实施统一的管控。涂鸦内部应用的服务访问都需要使用统一的客户端 Client 组件，通过该 Client 实现用户身份的相互识别和权限的控制。应用的鉴权通过统一的鉴权服务实现。

9.2.4 数据库权限管理

涂鸦的数据库权限管理主要包括：应用账号、数据库平台账号等。应用账号，是指提供给应用程序访问数据库使用的账号，通过对应用所在的机器标识，实现身份认证。

数据库平台使用的账号，由 DBA 专门创建，包括用于执行工单的读写账号和查询模块使用的只读账号等，数据库平台账号每 3 个月进行轮换。

9.3 供应关系安全管理

9.3.1 供应商评估

涂鸦针对平台软件供应商有严格的筛选机制和定期评估机制，除了硬件产品的安全指标，软件服务的安全标准，涂鸦更深入了解各个服务提供商在信息安全评估和隐私合规方面的实践。其中信息安全评估涉及安全渗透测试、供应商安全能力评估，具体可参照 5.4 节。

9.3.2 供应商服务质量监控

实时监控供应商的服务质量，关注供应商的安全资讯等，出现异常第一时间能够快速响应。

9.4 客户安全服务支持

涂鸦云平台完善的运营安全能力能够为客户提供云服务的 7x24 小时的全天候技术支持。

10. 终端安全

10.1 APP 客户端

10.1.1 客户端程序保护

客户端本身的安全往往是黑客突破 APP 客户端安全的第一道坎。从黑盒的思路，攻击者需要拿到客户端的源代码，然后对代码进行快速解读，包括查找特点的关键字或方法等，寻找漏洞。所以需要在这个过程增加一道门槛。除此之外，保护应用包不能被二次打包也是非常重要的手段。

涂鸦的 APP 客户端保护，包括针对客户端防篡改、代码混淆、模拟器检测拦截、Root 环境

检测告警、防止调试、界面劫持保护、Hook 插件检测和进程注入保护等。

10.1.2 组件安全

针对四大组件，Activity、Broadcast Receiver、Service、Conent Provider，严格限制组件的使用权限和访问权限，同时针对对外开发的组件，进行严格的权限和输入校验。

针对 WebView，保持 SDK 较高版本，针对 URL 域名和 file 访问权限进行严格控制。

10.1.3 数据安全

涂鸦 APP 客户端针对存放在客户端本地的数据，进行了严格的控制。

1. 内部存储：
    a) 私有目录：本地部分必须存放的配置文件等信息，通过安全的加密方式保存，同时密钥每个用户唯一，同时采用严格的读写执行权限设置。
    b) SQLite 数据库：不存储用户相关的敏感信息。
    c) 安卓的 SharedPreferences 配置文件：不允许出现敏感信息。
2. 系统日志：正式的客户端不打印和存放任何交互 logcat 或日志文件。
3. 密钥链数据：不硬编码重要的 Key。采用自主研发的安全算法保存密钥。
4. 内存数据：重要操作时候，用户数据不存入内存。

10.1.4 通信安全

1. 全链路通道 TLS 加密，包括 HTTPS 和 MQTT over TLS 等协议，严格校验证书信息，

避免劫持风险。

2. 传递的数据均内容使用 AES128 加密，同时加密的 Key 是基于每个用户生成的唯一的动态 Key。

10.2 硬件和固件安全

10.2.1 通信安全

根据不同硬件芯片的性能，涂鸦提供不同等级的加密机制，来最大化芯片的安全能力，不论哪种加密机制均保证数据的通信安全。目前涂鸦模组主要的通讯协议是 MQTT over TLS 和 HTTPS，均采用 TLS1.2 和 AES 双重加密保障，同时针对交互过程中的数据和控制指令进行额外的 AES 加密保护。TLS 采用双向身份和证书的强制校验，AES 加密密钥使用动态生成的基于设备的，具有唯一性的随机密钥。

同时，涂鸦所有通讯数据都会使用防重放校验、设备身份校验、访问控制和权限校验等多种数据保护机制。

10.2.2 固件保护

涂鸦针对固件进行多重保护：

1. 固件读写保护，根据芯片的平台支持程度，对固件的读写进行限制，防止通过硬件进行固件读取和写入。
2. 固件加密保护，部分平台本身支持固件加密，涂鸦均会启用，同时，针对核心代码，使用涂鸦自研的固件加密机制进行保护。
3. 安全启动，涂鸦会根据芯片平台的能力进行固件防篡改保护，支持核心代码或全部代码

的启动校验。

4. 固件防伪校验，涂鸦固件都会通过涂鸦的证书进行签名，云平台同时提供涂鸦固件防伪检测接口。

5. 代码混淆，对核心的代码进行额外的混淆和保护。

10.2.3 OTA 安全

涂鸦针对固件升级支持两种方式：完整的固件更新，和差分更新。涂鸦针对固件升级过程采取了多重保护手段进行保护：

1. 在生成固件包时，打包工具会生成一个固件完整性校验信息，该信息由多个变量组成。

2. 客户端请求固件时，服务端会下发一个固件下载信息和固件校验信息。该固件校验信息采用安全的 HMAC 签名算法，并且加入设备唯一的身份密钥信息作为因子，保证传输过程固件无法被篡改。

3. 客户端获取固件后，需要计算固件校验信息，并和服务端提供的固件校验信息进行对比，同时解压缩的时候还需要校验打包工具在固件内计算的完整性校验信息。只有完成固件双重校验后，才允许写入固件。

4. 固件如果写入失败，或写入后无法正常使用，会自动恢复到原有的固件。

10.2.4 数据保护

涂鸦联网模组提供安全芯片的支持，用来存放联网模组的授权信息和加密 key。授权信息用以保证对涂鸦模块和云端进行通讯的安全性和合法性，能够有效防止授权数据和加密 key

被非法人员盗取或篡改。安全芯片内部有安全数据区，在使用过程中，涂鸦模块会将加密的敏感信息读取到 RAM 中，掉电丢失。同时，模块和安全芯片通讯的时候，都会有临时密钥的加密保护。

非安全芯片版本，为了保障核心数据的安全，本地存储的重要信息，会进行 AES 加密后，存放。加密的密钥每个芯片初始化的时候随机生成，并安全存储，仅本地加密使用，不用于任何业务处理或进行任何交互。

10.2.5 配网安全

配网前的设备发现，APP 和硬件发出的广播信息，经过 AES 加密的传输。

配网过程中，APP 采用 AES 加密传输给硬件 WIFI 信息，保障了用户网络的安全，减小配网过程的风险。

11. 业务可持续性

11.1 业务持续性

为消除关键的生产经营活动出现中断，避免其遭受重大故障或灾难的影响，涂鸦通过运维平台对云平台所有的主机、应用、服务、网络等的实时监控，并且有一套完整的业务故障的自动化流程体系和保障，通过多服务热切换保障服务不中断。

针对业务系统软件硬件故障甚至天灾等非抗拒性因素导致的风险，规定了一套完整的应对方案，有能力保证在预知情况下的业务持续性。

11.2 灾难恢复

采用主从数据实时热备份、冗余存储和地备份的方式，保障业务数据安全可靠，持续可用。

并对对备份情况进行实时的监控和验证。

同时针对业务系统，多链路备用系统，保证能够快速应急切换。

11.3 应急方案

内部建立对各类型资产和安全风险的应急方案措施，以《涂鸦智能 IT 应急流程规定》为依据执行，能够保障事后能够正确、有序、高效地进行应急处理，保障工作的正常运转。应急方案包括了事前的预案流程、监控和一系列故障应对手段。事中通过详细的系统监控审查记录，为事后提供足够资料能够快速了解和分析，以及对应的接口人员。事后有一套完善的处理流程方法和应急预案，保障能够快速处理问题，分析问题和责任追责。

11.4 应急演练

定期实施大型的硬件故障、网络 DDoS、安全事件等内部技术应急演练测试和实战。

Prepared and Administered by Tuya Security Office.