涂鸦智能安全白皮书

Tuya Smart Information Security White Paper

Version 3.1.201912

Catalog

目录

1. 涂鸦智能介绍

涂鸦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 2019 年 10 月底，涂鸦智能已经服务全球超 18 万家平台客户，其中欧美非地区占比超五成以上，日语音 AI 交互超 4000 万次，独创完全中立的“AI+IoT”产品赋能模式。Powered by Tuya 赋能超 9 万款产品，赋能产品种数达到 500 种，全球第一，产品和服务覆盖超过 220 个国家和地区。

1.1 涂鸦云平台介绍

涂鸦在全球部署云服务，致力于为全球客户提供安全、稳定、快速的涂鸦云服务。涂鸦云拥有亿级海量数据和千万级用户并发处理能力，能够提供 99.99%服务可用性的不间断服务。通过整合亚马逊云、微软云等全球服务节点，涂鸦云可以为全球各区域的用户提供就近的访问服务，保障高效稳定的设备使用体验，助力中国制造服务全球！

平台拥有从产品定义、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的全生命周期服务能力。 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，可最大限度地降低硬件厂商的开发门槛，节约研发成本，提升厂商的智能产品研发速度。同时还能够帮助厂商进行软硬件智能升级，持续为最终消费者提供优质的服务。

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。

这篇白皮书从以下方面讨论了涂鸦云平台的各种安全防护措施：

1. 安全责任
2. 合规性
3. 数据安全
4. 云平台基础架构
5. 安全组织和人员
6. 云平台安全保障

7. 安全开发周期管理

8. 安全运维和运营

9. 业务安全和风控

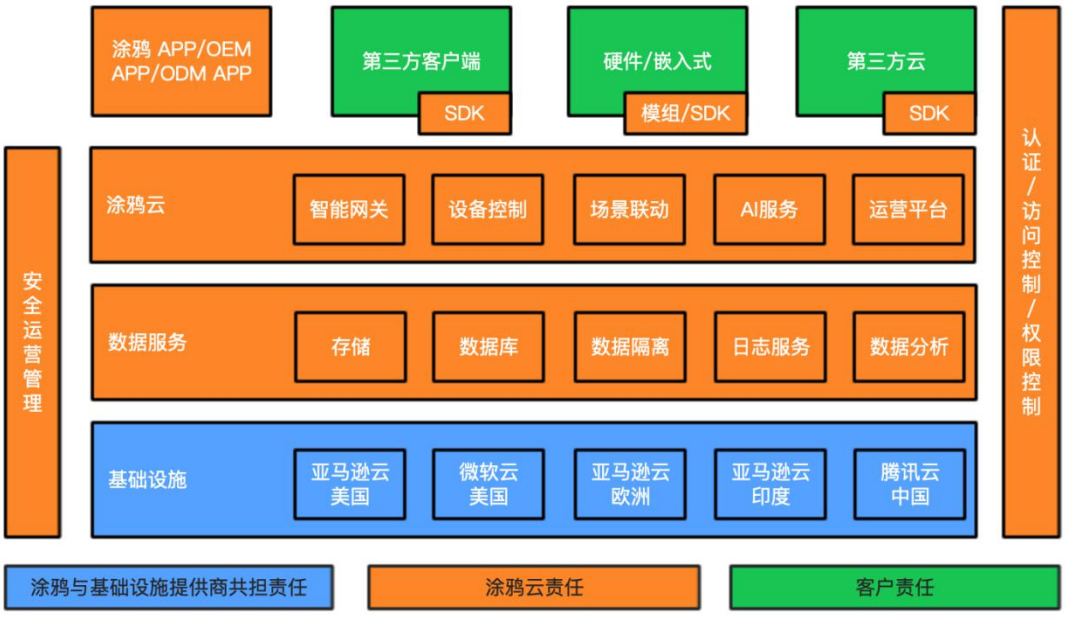
10. 终端安全

11. 业务可持续性

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. 合规性

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 27001

ISO 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 27017

ISO 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 27002 和 ISO 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 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 27018

涂鸦云获得了 ISO 27018 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 27018 是主要针对保护云中个人数据的实施规程。它基于 ISO 信息安全标准 27002，并针对适用于公有云个人可识别信息（PII Personally Identifiable Information）的 ISO 27002 控制体系提供了实施指南。它还提供了一组其他控制体系和相关指南，旨在满足现有 ISO 27002 控制体系组合未能满足的公有云 PII 保护要求。

涂鸦通过了 ISO27017&27018 这两个国际公认的行为准则，完成了 SGS 专家组的审核，这体现了涂鸦在云平台信息安全、尊重隐私和保护客户内容方面所做的努力。

3.4 ISO 9001

涂鸦智能已获得 ISO9001 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。

3.5 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 合规认证报告。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。

3.6 CCPA

涂鸦智能已通过 Trustarc 对涂鸦的 CCPA 审核。

加州消费者隐私法案(CCPA)将于 2020 年 1 月 1 日生效，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。

3.7 “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。

4. 数据安全

4.1 涂鸦云数据安全体系

涂鸦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。

4.2 数据所有权

涂鸦为客户定制的服务中，客户是数据控制者，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，在符合法律法规、《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。

4.3 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。

4.4 用户设备数据安全

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：

在设备与云端交互方面：

- 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。

在设备局域网内交互方面：

- 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。

此外，设备本身的安全保护，请参考 11.2 章节。

4.5 企业数据安全

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。

4.6 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。

4.7 隐私保护

涂鸦云平台践行“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。涂鸦以坚实的技术基础和完备的运营管理机制，确保用户和客户数据得到全面的保障。涂鸦云将严格执行涂鸦公开发布的《隐私政策》，切实保护用户隐私。

云平台对隐私数据的主要保护手段如下：

- 隐私数据生产和分类
  - 基本原则：
    - 信息收集主体的所有行为的合法要求，包括数据主体的授权和法律责任的明确。
    - 收集的数据最小化原则，不收集和提供的服务无关的数据。
  - 充分的用户知情权，
    - APP 和网站的隐私政策
      - 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。
      - 隐私条款必须在涉及注册、更新等重要时机通过邮件、APP 弹窗等方式告知用户。
      - 隐私条款必须包含数据收集、删除、迁移、保存、用户选择权等。

- 要求用户必须对隐私政策作出反馈。

◆ 网站 Cookie 声明

- Cookie 的作用及用户选择权。

■ 用户权限：

◆ 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，

◆ 被遗忘权（数据删除权）

- 账号注销权限和删除数据

◆ 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。

◆ 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。

■ 数据分类：区分个人数据和平台信息数据，针对个人数据，需要用敏感程度分类。

4.8 数据存储区域

- 五大数据中心：中国机房、美国西部 AWS 机房、美国东部 Azure 机房、和欧洲机房、印度机房（各数据中心之间物理隔离不互通）。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：数据保存在中国杭州 BGP 机房，由 Aliyun 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。用户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：数据保存在德国法兰克福机房，由 Amazon AWS 提供基础云计算支持。
- 印度：数据保存在孟买机房，由 Amazon AWS 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。

5. 云平台基础架构

5.1 云平台基础架构图

涂鸦云平台的基础设施由 AWS、Azure 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/cn/cloudapi/。

5.2 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 和 Azure 等。

6. 安全组织和人员

为了让所有员工不断提升安全意识，更好地保障客户利益和产品与服务信誉，涂鸦智能在公司内部倡导“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

涂鸦有专职和完整的安全技术团队，该团队来源于阿里、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

隐私安全合作机构做保证。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。

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，以遵守法规和合规性要求为基线，并为涂鸦（包括运营和业务利益相关方）提供风险和合规性支持。

6.2 人力资源管理

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。安全对 HR 的诉求主要是保证我们的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。

员工离职，会有严格的自动化和人工对于其电子设备、服务器、各种账号等资源的回收。

6.3 安全意识教育

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，了解手册上面的的政策和制度。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。

6.4 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，ISO 和等级保护等安全合规体系要的培训。

6.5 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。

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、美国西部、美国东部和印度五个可用区。

包含但不限于美国西部俄勒冈主机房；美国东部弗吉尼亚机房；欧洲法兰克福机房；腾讯云上海机房；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

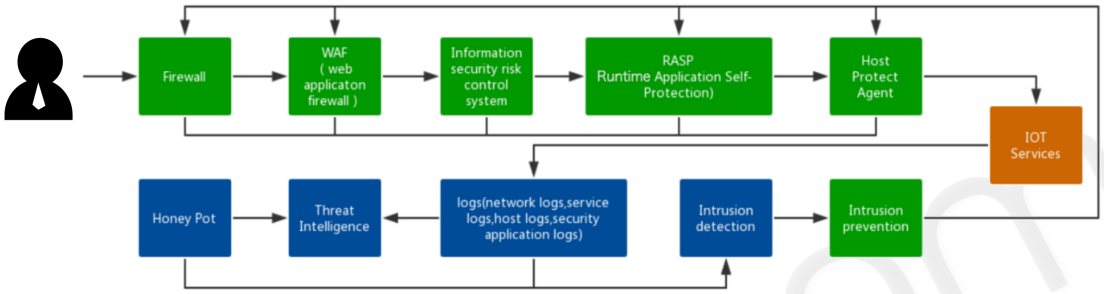
- 安全事件管理：和云服务器供应平台达成物理安全应急预案，并定期组织数据中心工作人员进行安全演练。一旦发生物理安全事件，该预案将能够立即生效并指导相关人员以最大可能保护客户资产。

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、入侵检测、RASP、主机防护系统等多重防护机制，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，且实施强制的证书认证的加密保护，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。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。

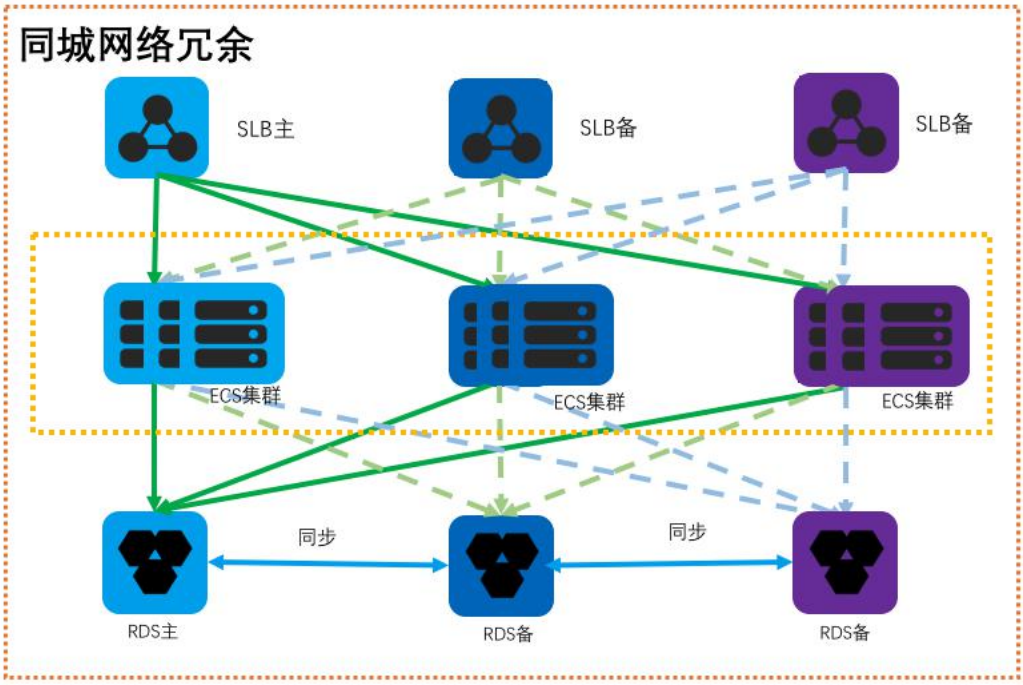
7.2.4 网络冗余

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

涂鸦云使用 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，保证云平台网络稳定。

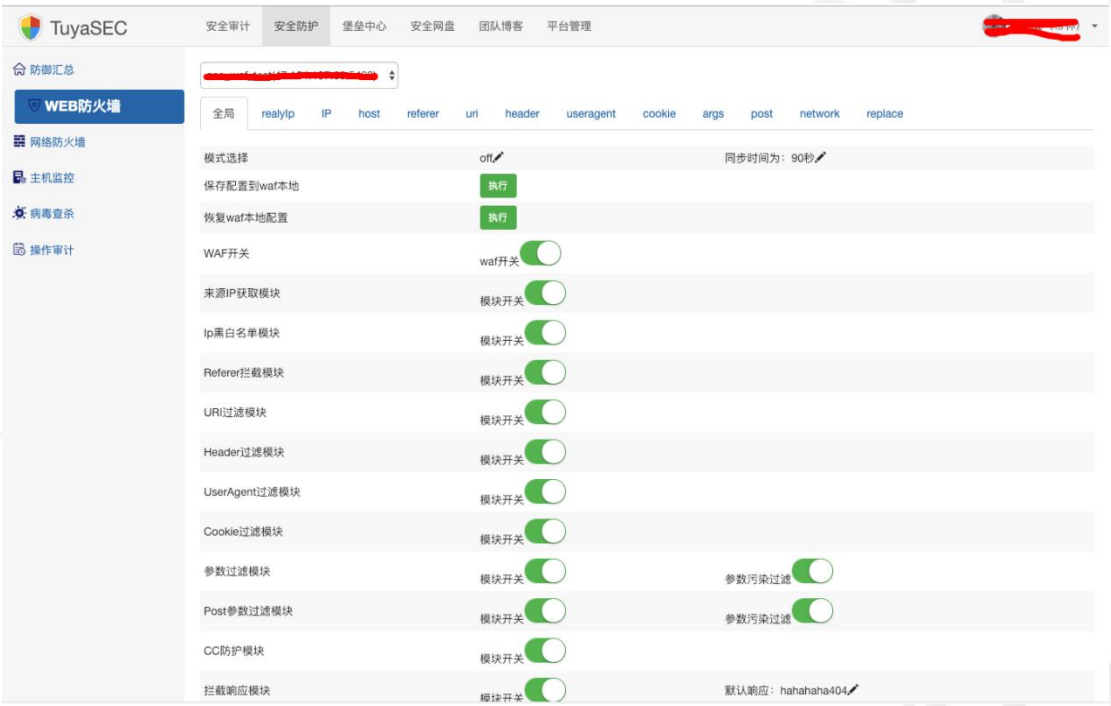
对于 CC 攻击，内部通过防火墙和 WAF 进行阻断。同时内部通过对所有请求日志的分析和结合第三方威胁情报数据，进行异常的 IP 进行检测，动态屏蔽可疑的源地址。

7.2.6 入侵防护

- 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。

- 入侵防护：通过防火墙和 WAF 等设备进行入侵阻断。



- 主机监控：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。

- 数据库审计：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。

- 病毒查杀：触发式检查，所有业务接口上传上来的文件。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。

8. 安全开发周期管理

严格按照安全开发生命周期方法开发云平台及云产品，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 SDL 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，形成《安全需求分析建议》，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，对产品设计中采用的技术进行安全评估，形成《产品设计安全建议》，并与开发人员就安全建议达成共识。

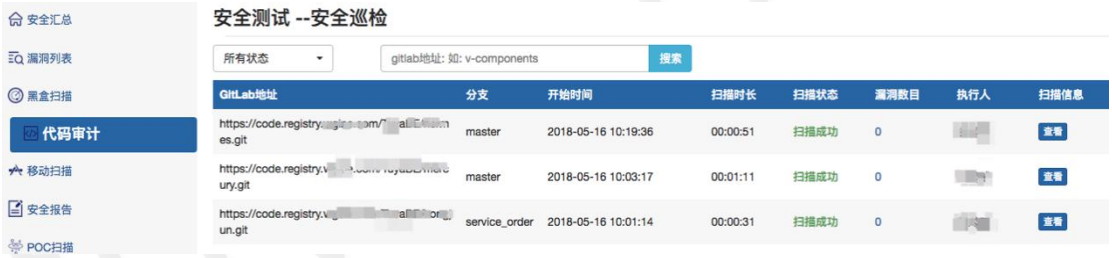
8.2 开发阶段

8.2.1 安全开发规范

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。

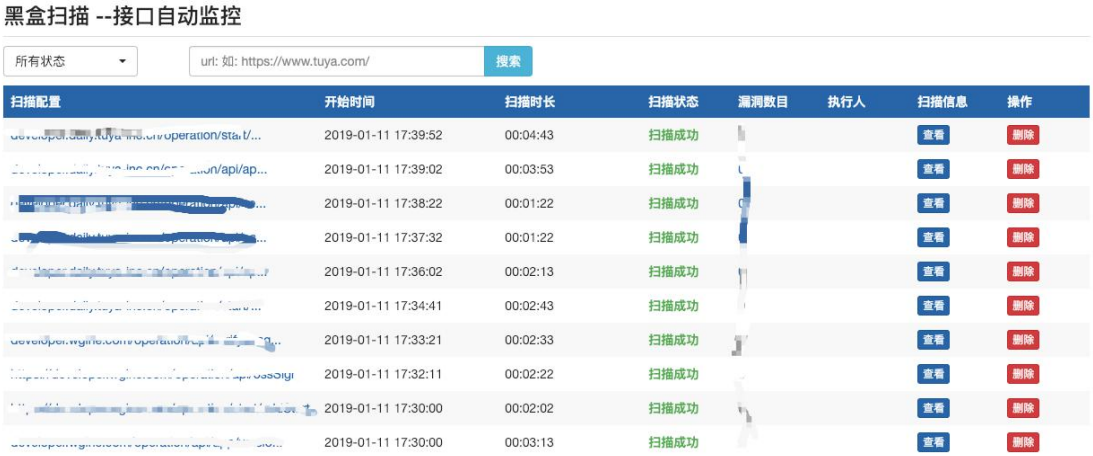
8.2.2 代码审计

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。自动化化实时跟踪主流漏洞情报，自动更新不安全的第三方组件库，能够第一时间生成规则进行漏洞告警。



8.2.3 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。



8.2.4 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。

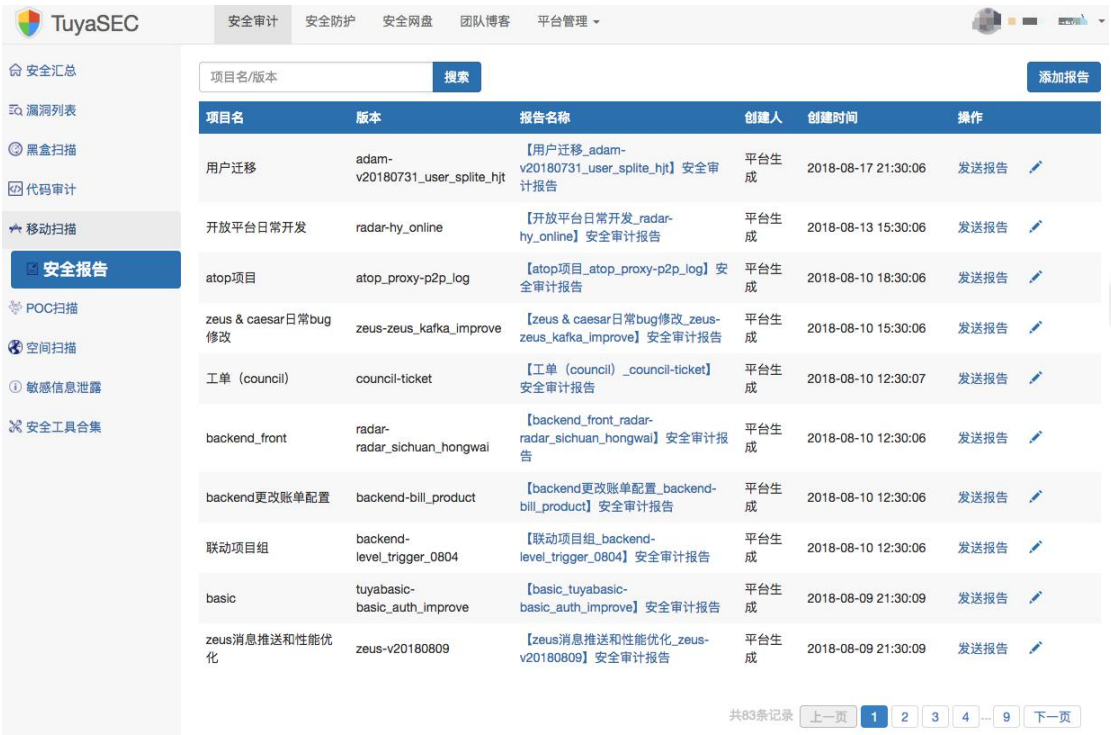
8.3 安全测试和修复验证

8.3.1 渗透测试

测试阶段，涂鸦安全团队通过漏洞扫描平台、代码审计工具、移动扫描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；

8.3.2 漏洞修复和渗透测试报告

发布阶段，只有经过安全测试并且得到《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

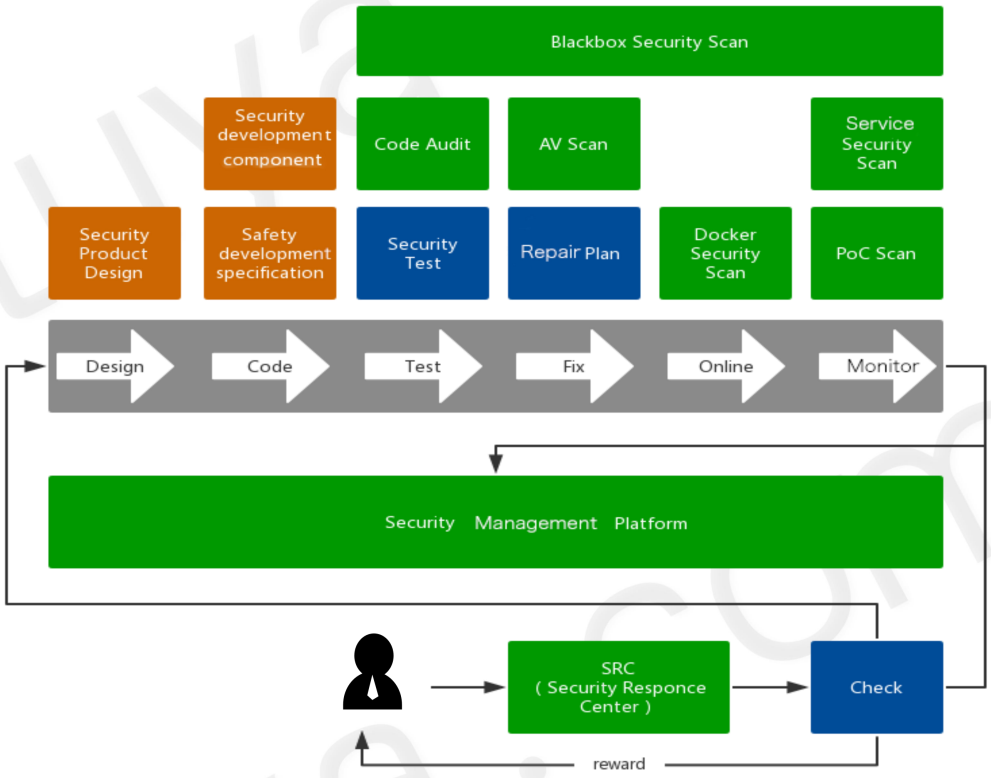
通过涂鸦的安全运维平台进行统一的管理，采取严格的访问控制、监控审计来确保运维安全。

- 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、硬件产品以及遍布整个企业的渗透测试。

涂鸦支持外部白帽子通过邮件等渠道提交漏洞，涂鸦会对外部披露和第三方安全服务公司的漏洞审计或举报结果，进行分类、严重程度排序和通过工单跟踪修复。

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。

针对紧急漏洞，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。

9.1.1 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、代码组件漏洞扫描等。

9.1.2 第三方安全渗透

至少一年 2~3 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。

9.1.3 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。

9.2 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. 业务安全与风控

10.1 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。

10.2 内容安全

专门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。

11. 终端安全

11.1 APP 客户端

11.1.1 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。

11.1.2 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。

11.1.3 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。

11.1.4 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。

11.2 硬件和固件安全

11.2.1 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。

11.2.2 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。

11.2.3 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。

11.2.4 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。

11.2.5 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。

12. 业务可持续性

12.1 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。

12.2 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。

12.3 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。

12.4 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。