



乐橙云安全及隐私保护白皮书

V1.0.0

杭州华橙网络科技有限公司

版权声明

© 2021 杭州华橙网络科技有限公司 版权所有。

在未经杭州华橙网络科技有限公司（下称“华橙”）事先书面许可的情况下，任何人不能以任何形式复制、传递、分发或存储本文档中的任何内容。

本文档描述的产品中，可能包含华橙及可能存在的第三人享有版权的软件。除非获得相关权利人的许可，否则，任何人不能以任何形式对前述软件进行复制、分发、修改、摘录、反编译、反汇编、解密、逆向工程、出租、转让、分许可等侵犯软件版权的行为。

商标声明

- 、、是杭州华橙网络科技有限公司的商标和/或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

- 在适用法律允许的范围内，在任何情况下，华橙都不对任何人因本文档中相关内容及描述的产品而产生的任何特殊的、附随的、间接的、继发性的损害或任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 本文档中描述的产品均“按照现状”提供，除非适用法律要求，华橙对文档中的所有内容不提供任何明示或暗示的保证。

出口管制合规声明

华橙遵守适用的出口管制法律法规，并且贯彻执行与硬件、软件、技术的出口、再出口及转让相关的要求。就本文档所描述的产品，请您全面理解并严格遵守国内外适用的出口管制法律法规。

关于本文档

- 您购买的产品、服务或特性等应受具体商业合同和条款的约束，本文档中描述的全部或部分产品、服务和特性可能不在您的购买或使用范围之内。
- 如不按照本文档中的指导进行操作，因此而造成的任何损失由使用方自己承担。
- 如获取到的 PDF 文档无法打开，请将阅读工具升级到最新版本或使用其他主流阅读工具。
- 华橙保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。
- 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以华橙最终解释为准。

概述

乐橙云安全及隐私保护白皮书，旨在呈现华橙对云安全及隐私技术研究与实践的成果，以便让广大用户更加清晰地了解乐橙云的安全和隐私保护能力。

名词解释

名词	说明
API	Application Programming Interface，即应用程序编程接口，是一些预先定义的函数，或指软件系统不同组成部分衔接的约定。
BIA	Business Impact Assessment，业务影响评估。
DevOps	Development 和 Operations 的组合同，是一组过程、方法与系统的统称，用于促进开发（应用程序/软件工程）、技术运营和质量保障（QA）部门之间的沟通、协作与整合。
RASP	Runtime application self-protection，运行时应用自我保护。
sSDLC	Secure Software Development Lifecycle，即安全软件开发生命周期。
STRIDE	Spoofing(假冒)、Tampering(篡改)、Repudiation(否认)、Information Disclosure(信息泄漏)、Denial of Service(拒绝服务)和 Elevation of Privilege(提升权限)，是一种威胁建模方法。
P2P	Peer-to-Peer，也叫对等互联或点对点技术。P2P 不是一种新的协议，而是利用现有的网络协议实现网络数据或资源信息共享的技术，它使用的可能是 TCP、UDP 或其他协议。
PIA	Privacy Impact Assessment，隐私影响评估。
PII	Personally Identifiable Information，个人可识别信息。
TSL	Thing Specification Language，物模型是一个 JSON 格式的文件，它是物理空间中的实体在云端的数字化表示。
VPC	Virtual Private Cloud，是公有云上私有网络，通俗讲就是用户可自定义的网络。
WAF	Web Application Firewall，Web 应用防火墙。

修订记录

编号	版本号	修订内容	发布日期
1	V1.0.0	首次发布	2021.03.08

目录

- 法律声明 1
- 前言 2
- 1 智慧物联-云战略 5
- 2 责任共担模型 7
 - 2.1 乐橙云责任 7
 - 2.2 用户责任 7
- 3 安全合规资质 9
- 4 安全组织和人员 12
 - 4.1 安全组织架构 12
 - 4.2 安全教育培训 12
 - 4.3 人员安全管理 12
- 5 云平台安全保障 13
 - 5.1 基础设施安全 13
 - 5.2 网络安全 13
 - 5.3 主机安全 14
 - 5.4 中间件安全 14
 - 5.5 安全及隐私设计 15
 - 5.5.1 云安全基线 15
- 6 应用与业务安全 17
 - 6.1 账号安全 17
 - 6.2 API 安全 17
 - 6.3 P2P 安全 18
 - 6.4 第三方视频加密 20
 - 6.5 客户端安全 20
 - 6.6 业务风控 20
 - 6.6.1 账户风控体系 20
 - 6.6.2 内容风控体系 21
- 7 数据安全及隐私保护 22

7.1	数据生命周期	22
7.2	数据隐私保护	23
7.3	媒体数据安全	23
7.4	企业数据安全	23
7.5	数据备份安全	24
7.5.1	多数据中心	24
7.5.2	多副本冗余	24
8	安全工程能力	25
9	安全运维&运营	26
9.1	特权账号管理	26
9.2	操作安全管理	26
9.2.1	容量管理	26
9.2.2	变更管理	27
9.2.3	威胁防御	27
9.3	安全日志及事件管理	27
9.3.1	日志分析与告警	27
9.3.2	事件管理	27
9.4	业务连续性	28
9.4.1	灾难恢复	28
9.4.2	应急预案	28
9.4.3	应急演练	28
10	安全承诺	29

1 智慧物联-云战略

随着 5G、AI 以及大数据技术的发展，“万物智联”成为未来产品的发展趋势。作为数字化时代下的重要基础设施，云计算凭借其高效性、扩展性、便捷性，为 AIoT 智能化、数字化转型提供了必要条件。

乐橙，是华橙于 2014 年创立的民用智慧物联网品牌。2018 年，为面向全球市场，海外品牌全面升级为 Imou。华橙以云平台为核心，构建以视频智能硬件、视频云、智能技术“三位一体”的业务生态，通过接入网络摄像机、智能门锁、无线探测感应器等智能设备，为家庭、商铺、小微企业，提供围绕用户场景的智慧物联服务。同时利用乐橙云开放平台，与第三方视频应用开发者分享云平台服务能力，帮助其开拓更多的场景化应用服务，共建智慧物联网云生态。

网络安全及隐私保护始终是华橙最高纲领和核心发展战略之一。华橙坚守“合规、开放、透明”的理念，秉持为用户提供高效、安全、可信视频云服务的初心，积极面对层出不穷的安全与合规挑战，基于纵深防御的安全理念，结合“默认安全设计”和“默认隐私保护设计”的设计原则，不断完善云安全保障措施，联动全领域安全能力，持续构建乐橙云安全及隐私保护框架。

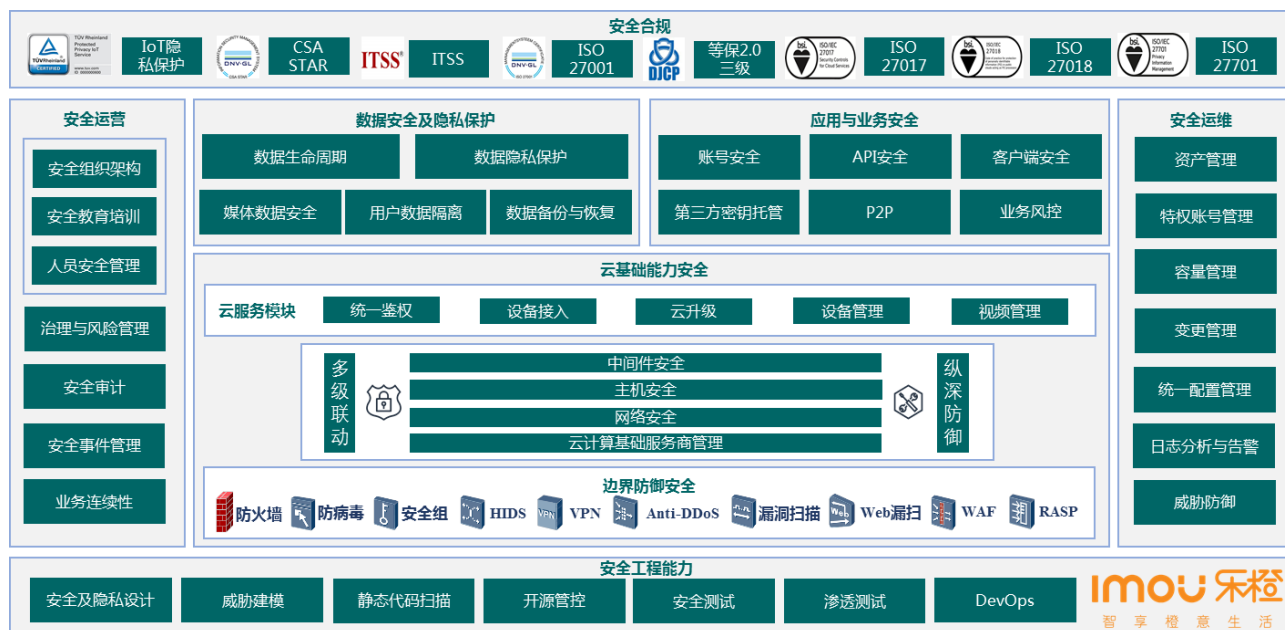


图 1-1 云安全及隐私保护框架

乐橙云针对云安全联盟（CSA）、OWASP 提出的核心安全问题¹，采用基于 STRIDE 模型的威胁建模方法，持续迭代地检测和分析安全风险，并针对性地制定消减措施，致力于达到云原生安全的目标。

本白皮书从如下几个方面介绍乐橙云的安全及隐私保护体系：

- 责任共担模型
- 安全合规资质
- 安全组织和人员
- 云平台安全保障
- 应用与业务安全
- 数据安全及隐私保护
- 安全工程能力
- 安全运维&运营
- 安全承诺

2 责任共担模型

乐橙云依托基础云服务提供商的“基础设施即服务 IaaS”能力，构建了以视频为核心的 AIoT 云平台能力，并基于此为用户提供电商平台、乐橙 APP、乐橙含光、乐橙云开放平台、IoT 等云服务。

下图为基础云服务提供商、乐橙云以及用户云安全责任共担模型：



图 2-1 责任共担模型

2.1 乐橙云责任

乐橙云依托云服务提供商的基础设施、物理、虚拟化和基础服务安全。通过签署服务协议，约束云服务提供商的安全管理；通过核查服务报告和开展尽职调查，检验云服务提供商的安全水平。

乐橙云提供云平台和服务的规划、设计开发、运维及运营安全，以保障用户数据和隐私安全。包括但不限于：

云平台与服务安全：使用安全标准化后的网络、主机、中间件、基础能力，构建安全的乐橙云平台；基于乐橙云平台提供的电子商城、乐橙 APP、乐橙含光、乐橙云开放平台、IoT 等服务的安全与合规。

数据安全: 业务数据在云服务环境中的全生命周期管理和隐私保护, 包括数据分类分级、安全隔离、访问控制、传输及存储加密、隐私脱敏展示等。

访问控制安全：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。

2.2 用户责任

乐橙用户在使用 SaaS 服务（电商平台、乐橙 APP、乐橙含光）时，需要关注云服务使用

安全，通过加强身份凭证和终端设备安全管理，以更好地保护个人数据安全。

乐橙用户基于乐橙云开放平台（包括使用 SDK）自行开发终端应用时，乐橙云仅对开放平台自身安全和保存到云端的数据安全负责，并提供技术支持。需要乐橙用户谨慎保障终端应用及数据的安全合规。

乐橙用户以物模型方式接入乐橙云时，需要严格按照乐橙云的安全配置和接入要求执行，以确保产品本身的安全性。

3 安全合规资质

华橙一贯高度重视并持续增加在提高客户信任方面的投入。通过业界通用的安全合规与标准遵从的认证，旨在提升乐橙云的整体安全能力和业务水平，提高客户对安全和隐私方面的信任。华橙始终秉持“以客户为中心”的核心价值观，将众多的合规控制点融入云平台内控管理和产品设计中。同时，积极参与行业安全标准的制定及推广，并以此建设和运行安全可靠的云服务。

在隐私保护合规领域，华橙遵循 GDPR 法案，落实隐私与数据治理实践标准，已通过德国 TÜV 莱茵 IoT 服务隐私保护认证和英国标准协会 BSI 颁发的 ISO27701、ISO27018 认证。

在云安全控制领域，华橙践行 CCM 云控制矩阵和 NIST SP 800-53 标准，已通过挪威船级社 DNV 颁发的 CSA STAR 认证和英国标准协会 BSI 颁发的 ISO27017 认证；

在信息安全管理领域，华橙遵循国际权威认证体系，已通过挪威船级社 DNV 颁发的 ISO27001 认证；

在网络安全及运营服务领域，华橙符合网络安全等级保护要求和 GB/T36326-2018《信息技术云计算云服务运营通用要求》，已通过了信息安全等级保护三级资质认证和 ITSS 云计算 SaaS 服务能力评估认证。



图 3-1 安全合规资质

● TÜV 莱茵 IoT 服务隐私保护认证

TÜV 莱茵基于欧盟 General Data Protection Regulation (GDPR)法案、德国联邦信息安全局（BSI）的 Cloud Computing Compliance Controls Catalog（C5）云安全标准和 TR-02102 加密技术指南，以及企业内部 2PfG 标准，为乐橙云提供 IaaS/PaaS/SaaS 层的物理安全、数据安

全、应用安全、网络安全，以及 APP 安全、安全开发流程、安全应急流程等全面评估服务，并开展了渗透测试验证。

华橙通过评估并获得 IoT 服务隐私保护认证，意味着乐橙云的网络安全和隐私保护能力达到行业领先水平。

● ISO/IEC 27701 隐私保护管理体系认证

ISO 27701 是国际标准化组织 ISO 和国际电工委员会 IEC 于 2019 年 8 月最新推出的，以 ISO 27001 和 ISO 27002 为基础，对信息安全管理体系（ISMS）在隐私信息管理方面加以拓展而形成的隐私信息管理体系（PIMS）。ISO 27701 通过建立、实施、维护和持续改进的方法对信息安全和隐私信息管理提出了极高的要求，并通过审核方式验证组织符合隐私信息管理体系的要求。从标准建立之初便考虑了对 GDPR 法案，以及 ISO 29100、ISO 29151 等其他隐私相关标准条款的映射，是业内公认最具权威性的隐私信息管理体系建设指导标准。

华橙通过 ISO 27701 隐私信息管理体系认证，对完善并提升乐橙云数据安全和隐私保护能力，以及加速全球安全合规体系建设具有重大意义。

● ISO/IEC 27018 云隐私保护认证

ISO 27018 云隐私保护认证是国际上第一个指导公有云服务提供商如何保护云用户个人可识别信息(PII)安全的国际标准，它提供了一组额外的控制措施和相关指导，旨在解决现有的 ISO 27002 控制措施及未解决的公共云 PII 保护要求。

华橙通过 ISO 27018 认证，标志着乐橙云的隐私保护符合国际公认的云中个人可识别信息的保护要求。

● CSA STAR 云安全国际认证

CSA - Cloud Security Alliance, STAR - Security, Trust & Assurance Registry, 在 ISO/IEC 27001 的基础上，结合云安全控制矩阵（CCM - Cloud Control Matrix）的要求，运用成熟度模型和评估方法，为提供和使用云计算的任何组织，从沟通和利益相关者的参与；策略、计划、流程和系统性方法；技术和能力；所有权、领导力和管理；监督和测量等 5 个维度，来综合体现云的安全管理和技术能力。

华橙通过 CSA STAR 认证，意味着乐橙云的安全能力已符合国际标准要求，在智能家居物联云服务领域获得国际权威认可。

● ISO/IEC 27017 云计算信息安全管理体系认证

ISO 27017 云计算信息安全管理体系认证建立在 ISO 27001 信息安全管理体系框架和 ISO 27002 作为良好的实践控制设置的坚实基础之上，为云服务提供商和云服务客户提供加强控制。ISO 27017 标准不仅提供了 ISO 27002 标准中 37 个控制基于云端的指导方针，而且还介绍了 7 个全新云控制以解决云端特有的问题。

华橙通过 ISO 27017 标准认证，证明乐橙云遵守国际公认的安全实践。基于标准要求，乐橙云将建立更加完善的云安全管理体系，提升整体云安全服务能力。

● ISO/IEC 27001 信息安全管理体系认证

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提供了最佳实践指导。华橙依据 ISO 27001 建立安全管理体系，确保产品/解决方案/云的安管理合规。华橙已通过被全球广泛采用的安全标准 ISO 27001 信息安管理体系认证，采用以风险管理为核心的方法来确保华橙和用户信息的保密性、完整性和可用性，遵循 PDCA 方法，并通过定期评估风险和控制措施实现体系的持续运行。

● 信息安全等级保护 2.0 三级认证

信息安全等级保护，是中国最权威的信息产品安全等级资格认证，由公安机关依据国家信息安全保护条例及相关制度规定，按照管理规范和技术标准，对各机构的信息系统安全等级保护状况进行认可及评定。其中三级是国家对非银行机构的最高级认证，属于“监管级别”。

华橙通过等保三级测评，意味着乐橙云在应对信息安全威胁时，具备等级保护定义的第三级信息系统所应具备的安全保护能力，包括安全对抗能力和恢复能力。

● ITSS 云计算服务能力评估三级认证

ITSS 云服务体系是以 GB/T36326-2018《信息技术云计算云服务运营通用要求》等国家标准为依据，围绕云计算服务中人员、技术、过程、安全、性能等关键要素而展开。内容分为“人力”、“运营管理流程”、“技术及性能”、“安全”、“运维管理”5个维度，26个建设点，全面覆盖了研发的各个领域。

华橙通过 ITSS 云计算服务能力 SaaS 三级认证，意味着乐橙云的云服务技能已获得国家权威机构的认可。

4 安全组织和人员

为了不断提升员工的信息安全与网络安全意识，保障业务的合规运营，华橙将相关安全要求贯穿至员工招聘、入职培训、上岗培训、持续培训、岗位变动和离职等各个环节，将安全工作落实到每一个人的日常工作中。

4.1 安全组织架构

华橙通过自上而下的安全组织机构，保证安全目标、安全策略和安全战略规划的一致，为有效落实云安全战略，推动乐橙云安全与合规建设提供所需的资源。

在组织管理层面，华橙设立网络安全委员会，该委员会在董事会领导下，直接决策和批准网络安全战略，负责全面领导、管理并监督网络安全有效实行。

在隐私合规层面，华橙聘请有丰富安全实践经验的数据保护负责人，负责数据安全和隐私保护事务。同时，成立了网络安全与数据保护合规小组，包括法务代表、网络安全代表、信息安全代表、市场代表、交付代表、产品线代表，持续对标业界领先法案和标准，以主动合规和持续内部审计的策略来提高产品的合规性和安全能力。

在安全技术层面，华橙设立专门的云安全团队，指导和评价乐橙云的安全设计、安全方案、关键安全技术、安全风险管理和安全运维工作，以及支撑安全事件的应急处置。

4.2 安全教育培训

华橙从意识教育普及、宣传活动开展、安全能力考核三个方面开展员工安全教育培训：

- 意识教育普及：定期开展全员信息安全意识培训及针对关键岗位人员的网络安全和隐私合规培训，要求员工了解公司的政策和制度，知晓个人需要负担的责任和义务，并承诺按要求执行。
- 宣传活动开展：开展形式多样的安全宣传活动，包括信息安全专项行动，安全与合规典型案例宣传等。
- 安全能力考核：通过员工学习平台，每半年度开展例行信息安全考试，传递公司在信息安全及隐私保护领域的要求，以此提升员工安全意识和能力水平。

4.3 人员安全管理

员工在入职时需签署员工保密协议、参加并通过信息安全考试。机要岗位人员需额外签署机要岗位保密协议。

华橙安全流程制度充分考虑落地执行，对过程的活动、角色、职责进行了明确的定义。遵循最小权限和职责分离原则，通过审批流程授予员工资源访问权限。在员工转岗或离职时，通过加签工单审核节点，确保权限及时回收。保存完整的过程记录，供安全团队定期审计。

5 云平台安全保障

5.1 基础设施安全

乐橙云依托亚马逊云 AWS、微软云 Azure、阿里云等全球知名云服务提供商的基础服务，构建了乐橙云全球服务节点，通过管理和技术手段提高基础服务的稳定性。

- 供应链安全管控：设定云服务提供商安全能力与资质门槛，严格把控准入条件，不定期开展尽职调查，检验各云服务提供商安全报告，确保基础设施的安全性与可靠性。
- 高可用架构：采用多云厂商互备的策略，校验云厂商之间的可移植和互操作性，以快速应对部分云服务提供商不可用的情况。为主要服务模块部署多台服务主机，配备负载均衡系统，部署多个服务节点，在部分服务器宕机时不影响业务功能正常使用。

5.2 网络安全

乐橙云整合防火墙、安全组、云 WAF、RASP 等多重防护机制，采用 VPC 网络部署方式构建网络安全架构。VPC 对等连接功能保障了多个区域节点之间的数据传输安全，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，乐橙云可实现细粒度的网络隔离需要。

- 访问控制：通过安全组强制默认拒绝规则，开启 IP 白名单，限制到具体 IP 和端口，只允许可信的请求通过可信网络访问。
- 网络隔离：管理网络与业务网络逻辑隔离。内部管理系统使用堡垒机统一管理，服务器 SSH 端口及业务管理后台只对堡垒机开放，业务网络无法访问管理网络。
- DDoS 防护：乐橙云使用云服务提供商的 DDoS 防护功能，自动检测、调度和清洗，确保云平台网络稳定。结合防火墙和云 WAF 对恶意攻击流量进行阻断。

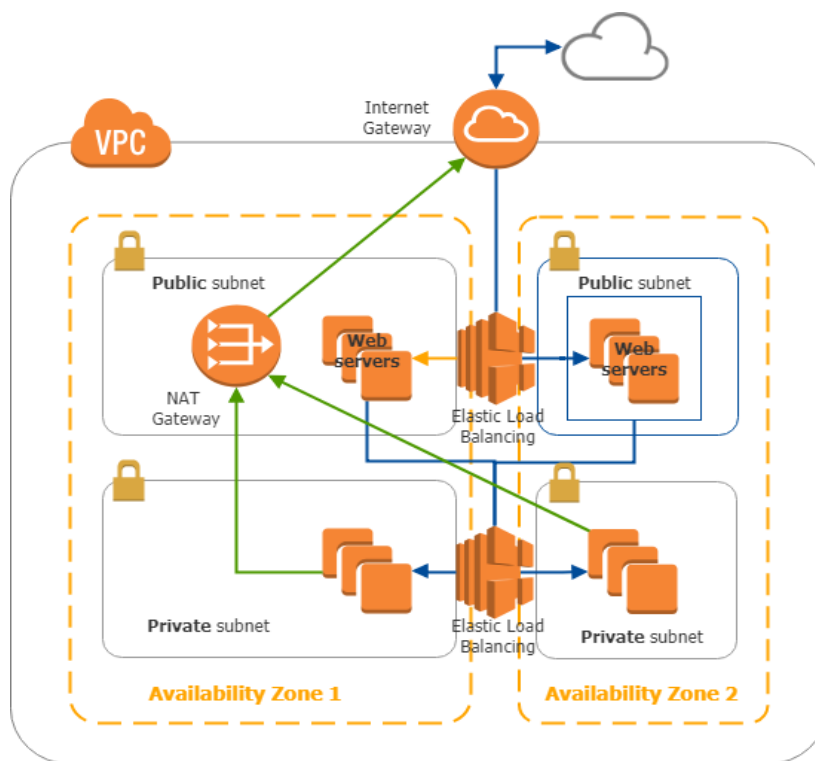


图 5-1 VPC 网络划分

5.3 主机安全

严格限制云主机的访问权限。在操作系统层面，构建了加固、检测、修复能力。

- 安全镜像：采用云服务提供商官方安全镜像，定期更新系统补丁、主机密钥。
- 系统加固：统一采用密钥登录，加固系统与服务配置，限制开放端口、安装服务最小化。
- 恶意程序检测：重要业务主机部署了防病毒软件，实时监控主机安全状态，定期对主机采取全盘病毒和木马扫描，并对恶意程序进行查杀。
- 关键文件变更检测：实时监控系统关键文件（如：开机加载、网络配置、`crontab` 任务、`passwd`、`sudoers` 配置等），一旦文件被修改即触发告警。
- 资源监控：实时监控主机资源容量情况，若超出事先设定的阈值，即触发告警。

5.4 中间件安全

为保障应用程序的运行效果和用户体验，使用了多种开发框架、中间件、数据库等。乐橙云从如下几个方面兼顾安全与性能的平衡。

- 安全选型：在选型时遵循软件准入原则开展安全评估，评估覆盖业务必要性、替代方案、维护更新情况、安全能力和合规水平。开源软件遵守开源管控要求。
- 安全加固：及时升级至较新版本，修复安全漏洞，开启安全功能、删除默认页面和禁用不使用的组件等。
- 凭证安全：登录凭证最小化权限处理，且要求不同项目使用不同的登录凭证。
- 访问控制限制：基于角色的访问控制策略，不同角色分配不同的访问权限。

5.5 安全及隐私设计



图 5-2 乐橙业务及安全设计

乐橙云安全及隐私设计覆盖规划、设计开发、运维和运营服务全过程，贯穿内部和外部多层防护，保障云服务核心业务和数据安全。内部防护机制，安全基线和专项加固以互补形式重点提升服务自身基础安全能力；外部防护机制，防护引擎可直接集成部署用于提升服务安全和动态防御能力。

结合 CIS 标准和业界优秀实践，乐橙云已具备 Struts2、Springboot、Docker、Nginx、RabbitMQ、ActiveMQ、Tomcat、MySQL、WEB 安全加固能力。并采取统一标准化进行要求。安全加固以标准安全理念为指导，降低组件攻击面，增强防御能力。

目前已正式发布《云安全基线》、《运维安全基线》、《客户端安全基线》，并持续迭代升级。配套发布《隐私保护规范》和《密码算法使用规范》，统一规范数据敏感等级及对应安全管控要求，加密算法和强度使用规则。

5.5.1 云安全基线

乐橙云实施“安全基线”计划多年，坚持以“Security by Design”和“Security by Default”为核心原则，深耕云安全技术，为用户提供充足的安全保障。

安全基线立足并践行安全与隐私设计原则，构建“AAA+CIA+P”的安全要素布局，形成覆盖系统安全、应用安全、数据安全、网络安全和隐私保护的系统化保护框架。

“AAA+CIA+P”安全要素布局具体为：

- AAA：认证（Authentication）、授权（Authorization）、安全审计（Audit）
- CIA：保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）
- P：隐私保护（Privacy Protection）

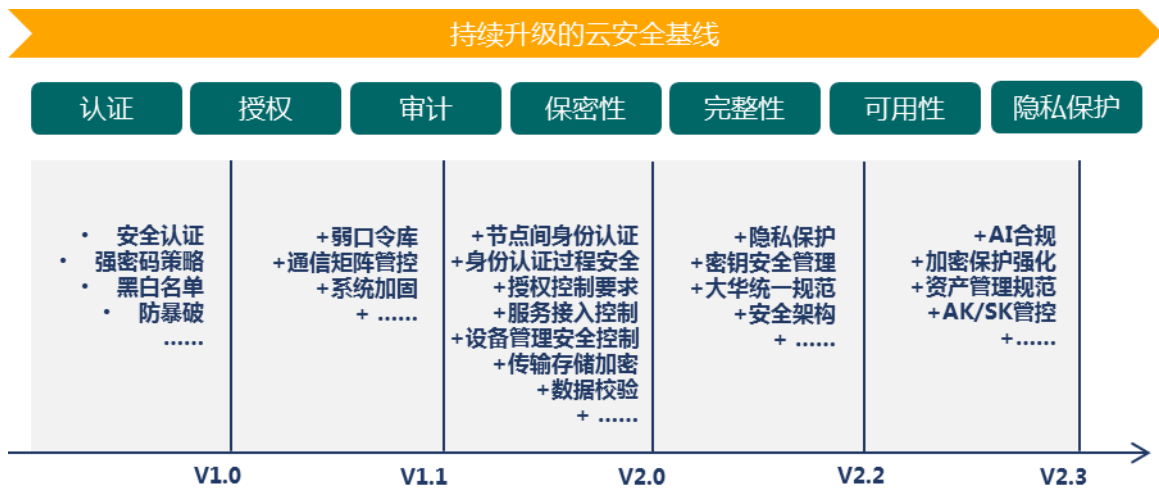


图 5-3 云安全基线

安全基线作为华橙的重要企业标准之一，是安全开发生命周期的重要组成部分，已融合到研发质量保障体系中，帮助乐橙云遵循安全管控要求、落地技术措施。

6 应用与业务安全

乐橙云在应用架构设计、应用部署中实施安全增强措施，乐橙云应用在开发、测试、上线过程中遵守企业安全标准，以安全合规为基础，充分考虑用户体验，提供个性化的应用服务。

6.1 账号安全

乐橙云针对账号注册、账号登陆、密码找回、账号注销等环节的风险场景制定了账号安全的相应管控策略和技术方案。

- 默认使用强口令策略，包括对口令长度、复杂度以及集成弱口令库等限制。
- 基于 Digest 认证，Digest 认证技术是一种挑战式的认证方法，基于对密码和随机数（一次有效）的 HASH 运算，确保认证过程的机密性和不可重放性。
- 传输过程使用标准 HTTPS 加密通道。
- 集成第三方验证码，自动识别用户账户攻击行为，通过拖动滑块等方式，防止机器批量注册，批量撞库登录等风险。通过 AI 等技术手段，识别非用户行为，定点锁定用户账户。
- 通过二次短信校验帮助用户找回密码。
- 注销后及时删除用户个人数据及关联数据。

6.2 API 安全

乐橙云整体采用微服务架构设计，提供标准的 RESTFul API 接口。考虑到 API 对云服务承载的重要功能和其在 HTTP 应用层面面临的安全威胁，乐橙云采用多重机制和安全措施对 API 进行重点保护，包括：

- 认证鉴权：乐橙云的 API 请求都会通过与后端的 IAM 服务进行身份验证，仅允许经过鉴权的用户访问相关信息。用户通过 API 接口来管理账号下的 IoT 设备，所以乐橙云对不同 API 或者 API 中包含的执行命令进行二级权限管理。当用户调用 API 管理设备时，不仅需要通过 IAM 的认证鉴权，还需要对命令的执行权限进行校验。当前的认证方式支持 token 认证和 AK/SK。
 - 1) Token 认证：认证请求会包含一个认证的 token，该 token 值由用户通过使用用户名及密码调用 IAM 接口获取。在 Token 获取之前，乐橙云集成了第三方防人机、防暴力破解工具作为获取 token 的前置条件。
 - 2) AK/SK：请求会包含 AK/SK 鉴权信息，用于游客模式的用户请求处理。
- 签名摘要：乐橙云采用金融级加密方案对每个 API 请求进行加密。并且在签名摘要的计算过程中融入了防重放攻击、防暴力破解，提升接口调用的安全性。

- 传输保护：API 调用时使用 TLS 加密以保证传输链路的机密性。并且支持 IoT 设备和乐橙客户端对乐橙云平台证书进行校验，确保 IoT 设备、客户端连接的安全性。
- 流量观测：乐橙云采用了云 WAF、API 频率检测、流量染色等技术提高用户访问乐橙云的高可用性和稳定性。
 - 1) API频率检测：为用户的API接口制定次数配额和调用频率阈值。一旦用户的请求次数/频率发生异常，会立即产生报警消息并通知相关人员进行处理。
 - 2) 流量染色：支持API请求灰度上线，对将流入的API请求进行分类，指向指定的后端灰度服务。

6.3 P2P 安全

乐橙云支持 P2P 技术，P2P 技术提供了用户通过公网远程安全地访问部署在局域网内的设备，实现设备点对点服务，提高资源利用率和访问效率，降低云服务运营成本，推动 IoT 互联互通能力。然而，利用 P2P 技术提升用户体验，推动物联网节点互联的特性时，对保障 P2P 服务架构体系的自身安全性也带来了极大的挑战。以下结合资产识别和安全控制来阐述 P2P 安全防御体系。

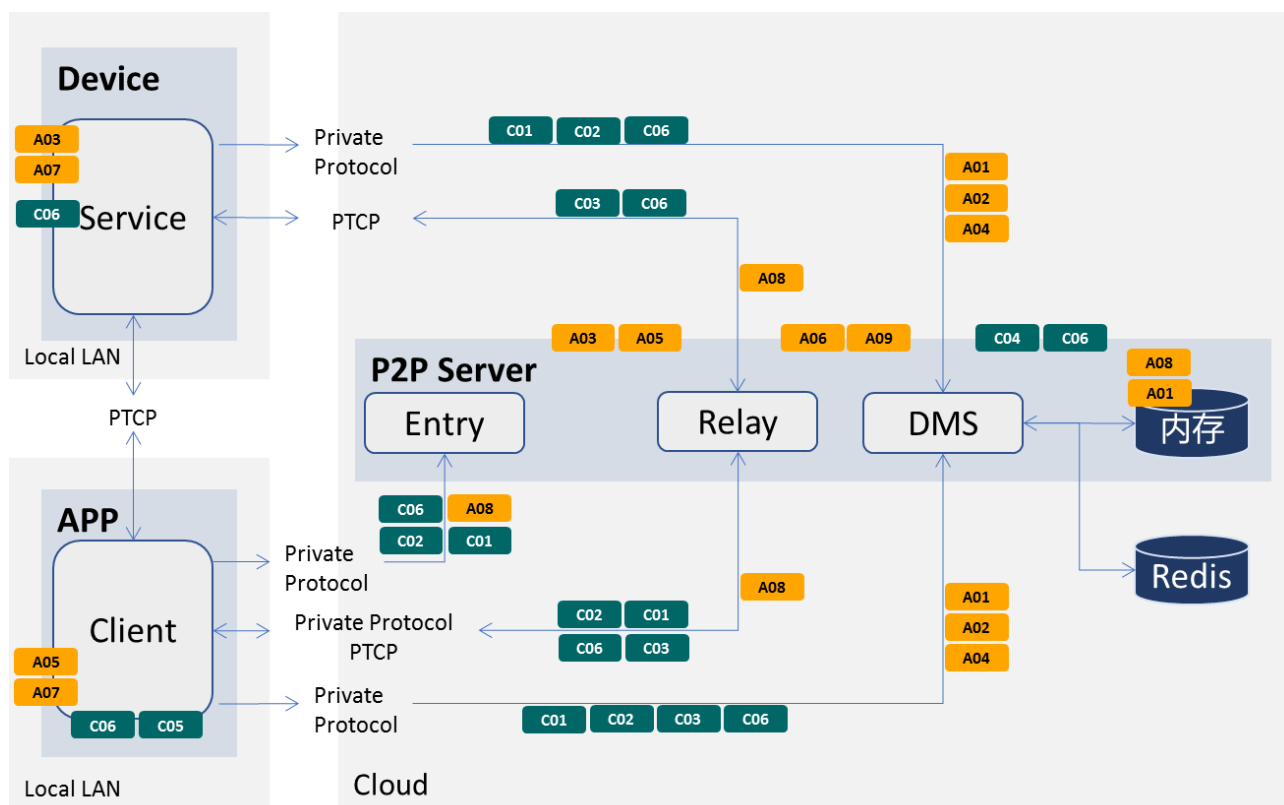


图 6-1 P2P 安全策略

- 资产识别
 - 设备信息（A01）：设备信息是建立 P2P 业务通道所必须的与设备相关的信息，其中包括设备唯一标识，设备公网地址和设备业务服务端口。
 - 设备公网地址（A02）：在客户端请求与设备建立 P2P 通道的触发下，设备动态建立外出公网地址，该地址代表了穿越 NAT 访问设备的一个通道，以供客户端与设备建立点对点访问通道。
 - 设备准入凭证（A03）：P2P 云服务器为了防止恶意使用者滥用服务资源，出厂时为合

法设备植入了准入凭证，只有拥有该凭证的设备，才能注册到 P2P 云服务端，确保接入设备的身份可信。

- APP 公网地址 (A04): 在用户期望通过 P2P 访问设备时, APP 主动建立外出公网地址,该地址代表了穿越 NAT 访问 APP 的一个通道,用于和设备建立点对点访问通道。
- APP 准入凭证 (A05): P2P 云服务器为了防止恶意使用者滥用服务资源, APP 发布程序中携带了 APP 准入凭证,只有拥有该凭证的 APP 才能接入 P2P 云服务并使用云服务资源,保证接入 APP 的身份可信。
- 传输加密服务器私钥 (A06): 该私钥属于服务器专有,用于和设备及 APP 建立加密通信通道使用,即在建立加密通道时协商对称加密密钥,该私钥是加密通道的信任根。
- 传输加密客户端私钥 (A07): 该私钥属于设备端或APP专有,用于和设备及APP建立加密通信通道使用,即在建立加密通道时协商对称加密密钥对称加密密钥,该密钥在系统中是有设备端或APP动态生成,而非固定长久保存。
- 转发节点绑定凭证 (A08): 当P2P打洞失败的情况下,为了保证两端通道依旧能够建立成功, P2P服务实现了转发业务,每一个通道都拥有一个专属节点,代表了双方通信的专属通道,而转发节点绑定凭证是用于保护通道使用权,不被恶意攻击者利用转发节点访问私网中的设备或APP。
- 服务资源 (A09): P2P服务资源是指云端的服务计算能力、内存等用于服务所必须的基础能力,该资源支撑了相应体量的P2P服务能力,也是云服务提供商的基础运营成本。

● 安全控制

- 准入控制机制 (C02): P2P 云服务扩展了 WSSE 认证机制对设备和 APP 进行准入控制,WSSE 利用了时间戳、准入凭证、随机数等的 HASH 计算,实现身份认证的同时,保证消息的不可重放性和保密性。
- Relay 点对点凭证校验 (C03): 由于网络环境限制,会存在一些场景打洞失败的情况,无法实现点对点交互, P2P 服务云提供了交互中转能力,为了避免恶意攻击者利用该转发节点,穿透目标设备或 APP 所在 NAT, Relay 节点设计了身份凭证校验机制,保证 P2P 转发通道合法用户才能实现数据转发。
- Dos 告警通知 (C04): P2P 服务云内部将会实时监控服务运行状态,当发现以下(不限于)异常状态时,将会通知运维人员,以保证及时处理服务异常:内存异常、CPU 异常、存储异常、服务异常、流量异常。
- 代码模糊化 (C05): 为了保护 APP 程序的一些保护逻辑机制不被恶意攻击者研究,我们对 APP 的固件进行了代码模糊化处理,提高逆向攻击成本。
- 数据校验 (C06): APP/设备/P2P 服务云的数据交互,都有严格的数据校验,避免恶意攻击利用非法参数对程序或服务进行攻击,实现内存溢出、代码注入等攻击模式。

6.4 第三方视频加密

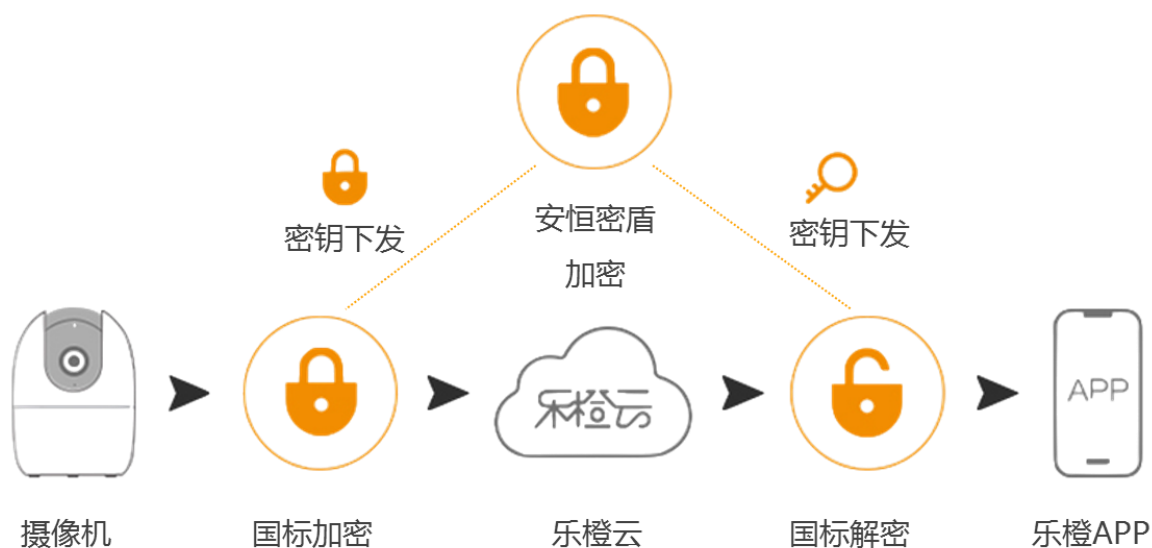


图 6-2 第三方视频加密

为满足用户对视频数据私密性的需求，乐橙云推出了第三方视频加密服务。协同安恒密盾生成加密密钥，对视频数据进行端到端加密。采用国密标准算法（SM2、SM4），视频传输实现全链路协同加密，全面保护用户数据安全。

乐橙用户使用第三方视频加密服务后，华橙、安恒都无法单独对加密后的视频进行解密。

6.5 客户端安全

遵循国内外法律法规、业界标准、部门监管等要求，乐橙的移动客户端落实了如下安全防护和隐私保护措施。

- 安全防护：包括客户端防篡改、防止权限滥用、防止调试、Root 环境检测、界面劫持保护、进程注入保护、“Activity、Broadcast Receiver、Service、Content Provider”四大组件安全设置、代码混淆、日志安全管理等。
- 隐私保护：包括隐私政策文本及集成要求、个人信息收集合法透明及最小化要求、权限申请明确告知及最小化要求、针对第三方 SDK 的合规审查、对用户权利的保障、隐私友好设置等。

6.6 业务风控

6.6.1 账户风控体系

具备识别登录终端设备变化、地理位置变化、频繁登陆等异常行为的能力，提示用户确认操作的真实性并记录登陆日志，以避免用户账户被盗用，滥用等风险。

6.6.2 内容风控体系

使用业务文件类型识别和病毒扫描、木马扫描引擎，识别上传文件的安全风险。

通过集成第三方内容过滤机制，识别色情、暴恐、涉政、广告、辱骂等违法违规字样，并且能够结合行为策略管控灌水、刷屏等恶意行为。

7 数据安全及隐私保护

7.1 数据生命周期

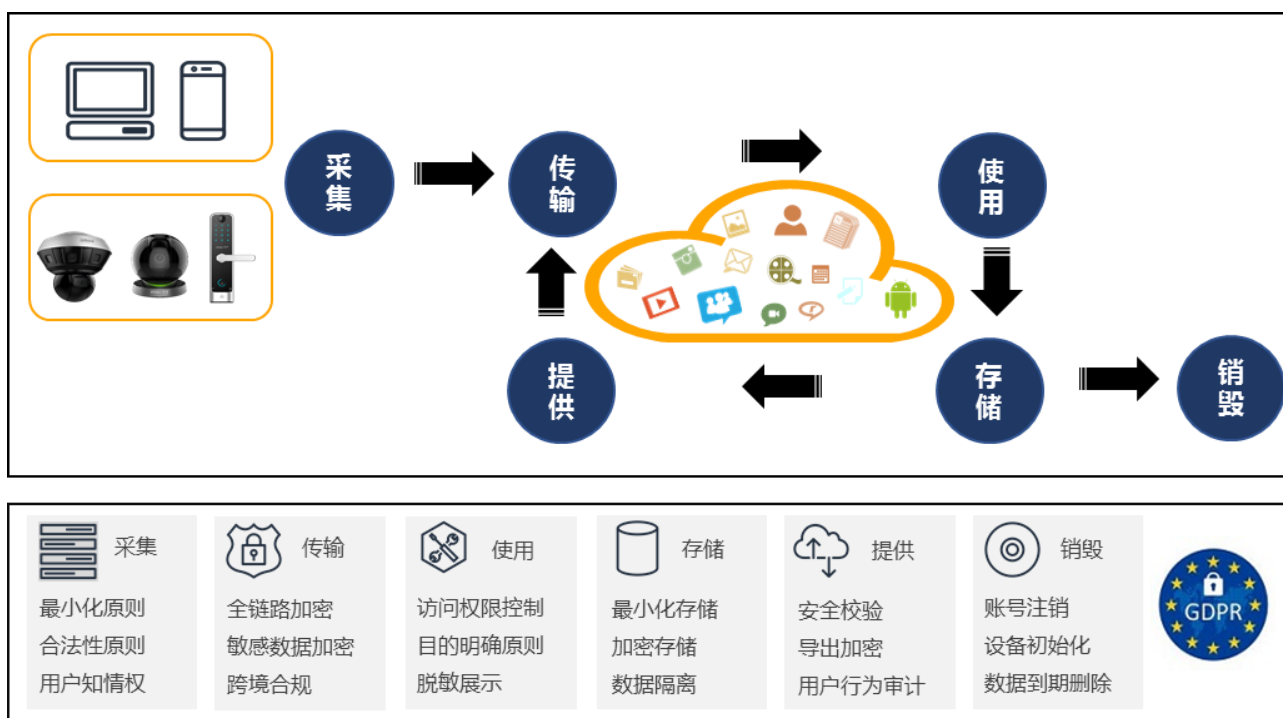


图 7-1 数据生命周期

乐橙云通过对数据全生命周期（采集、传输、使用、存储、提供、销毁）的安全管控，提升数据的保密性、完整性、可用性、隐私合规，保障云平台安全稳定运营。

- 采集：
 - 乐橙应用及设备，包括 IoT 设备（乐橙摄像头、智能门锁、无线探测感应器等）、APP 应用程序、PC 客户端、小程序等，遵守法律法规要求，评估业务功能逻辑，严格控制数据采集的范围、频率和精度。
 - 通过隐私政策告知用户，并获得同意和授权。
- 传输：
 - 传输通道使用 TLS 加密传输协议。
 - 提供口令在传输过程中内容加密的增强能力。
 - 慎重处理数据跨境的情况，通过调研对应区域及国家的法律法规，开展隐私影响评估，签署数据处理协议等方式确保合规遵从。
- 使用：
 - 实施细粒度的访问控制策略，仅授权人员鉴权成功后可访问数据。
 - 处理过程中，遵循收集时所声称的目的或合理关联的范围。
 - 展示个人敏感信息时采取脱敏处理，避免数据被非法访问或使用。
- 存储：

- 用户个人数据存储期限遵循最小化原则，处理目的完成后及时删除。
- 媒体数据存储依托云服务提供商的落盘加密存储能力，个人可识别信息（PII）实现 AES256 加密后存储（口令采用 HASH 加盐后存储），加密密钥（因子）可由用户设置。
- 普通数据和敏感数据分表存储，数据访问权限控制在表级别，以实现数据的逻辑隔离。
- 提供：
 - 使用乐橙 APP 的安全导出功能或联系官网客服，通过身份校验后可导出用户注册时提供的个人数据。
 - 提供用户使用自定义密码功能对导出数据进行加密。
 - 支持对发起导出数据的请求进行用户行为审计。
- 销毁：
 - 提供易于操作的注销账户功能，用户还可以联系官网客服清除云上个人数据。
 - 在使用乐橙摄像头等终端设备时，用户通过恢复出厂设置功能可以删除存储在设备中的个人数据，增加数据删除处理的透明性。
 - 在用户注销账户或者数据到期时，及时删除用户的个人数据或匿名化处理。

7.2 数据隐私保护

华橙践行数据隐私保护功能化、场景化，秉承隐私保护“合法性、公正透明、目的限制、数据最小化、准确性、存储限制、适度安全”原则，尊重用户“知情权、访问权、修改权、遗忘权、限制处理权、可携权、拒绝权、自动化决策与数据画像有关的权利”，采用业界认可的 Privacy by Design, Privacy by Default 理念作为指导，结合在数据隐私保护领域多年的经验沉淀，形成《产品隐私保护设计指引》。乐橙云已应用该指引开展隐私需求设计和隐私功能管理，同时，通过开展隐私保护影响评估（PIA），识别隐私风险并采取处置措施消除或降低风险。

目前，乐橙云已支持隐私模式、乐橙云解码、第三方视频加密、账号信息导出等隐私保护功能。通过《隐私政策》以及客户反馈通道，帮助用户了解乐橙云隐私保护能力。

7.3 媒体数据安全

当用户购买乐橙云存储服务，乐橙设备产生的报警录像将被存储在乐橙云上，供用户随时随地查看。乐橙云对上云的录像采取全生命周期安全防护：

- 录像上传：对媒体流进行内容加密，并具备支持基于 HTTPS 协议的传输加密能力。
- 录像存储：加密后的录像数据再次经过落盘加密存储于云存储中。
- 录像下载：客户端必须经过鉴权后才能下载录像。

7.4 企业数据安全

乐橙云对归属于不同企业客户之间的数据逻辑上禁止互相访问以实现安全隔离，并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数据，针对不同的业务场景提供不同的数据存储服务，对敏感数据采用 AES256 等加密算法进行加密存储，同时对加密密

钥采用统一的安全管理和分发机制。

7.5 数据备份安全

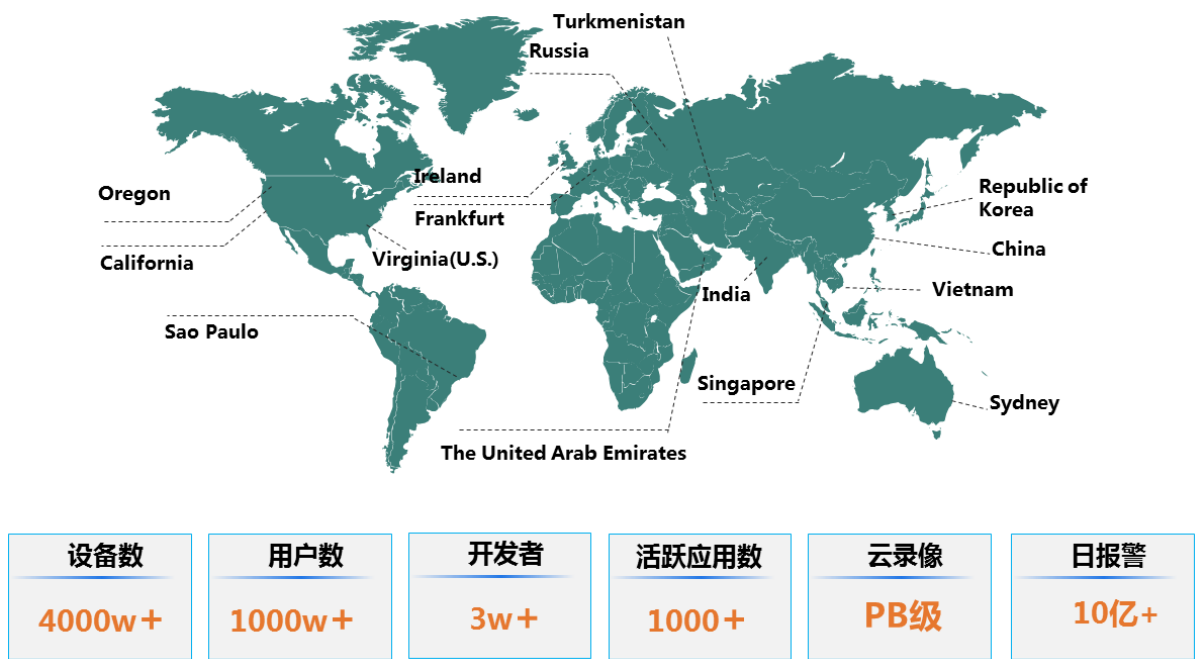


图 7-2 数据存储中心

7.5.1 多数据中心

乐橙云采用高可用策略，基于分布式架构，部署了中国（国内）、美洲（海外）、欧洲（海外）、亚太（海外）四大可用数据中心，乐橙云灵活地将数据和系统部署于不同数据中心或不同区域，根据用户所在地区提供相应的数据服务，以保证业务的容灾性。

- 中国数据中心：中国杭州机房
- 美洲数据中心：美国俄勒冈机房
- 欧洲数据中心：德国法兰克福机房
- 亚太数据中心：新加坡机房

7.5.2 多副本冗余

用户的音视频和图片数据采用多副本模式存储在云存储中，基于云服务提供商的 SLA 进行服务保障。结构化数据存储于加固后的数据库中，采用多副本模式（至少保证两个副本）每日自动全量备份，通过定期的应急演练检验备份的完整性和可用性。

8 安全工程能力

乐橙云在 sSDLC 安全开发生命周期管理实践过程中积累了安全工程能力和安全管理经验, 结合持续集成, 持续交付, 持续部署模式, 积极推行快速迭代的 DevOps 流程, 并引导 DevOps 逐步向 DevSecOps 演进。



图 8-1 安全工程

用户管理：

- 系统对接 LDAP 域账号，统一认证入口。

项目管理：

- 采用主流工具为项目提供需求管理、任务管理、wiki 等功能，准确把控每个迭代进度。
- 根据业务场景、数据流图进行威胁建模。当识别出威胁后，安全团队会根据消减库制定消减措施，并完成安全方案设计。威胁消减措施最终将转换为安全需求、安全功能。

代码管理：

- 支持 SVN、Gitlab 代码仓库服务。
- 研发代码遵循对内发布的安全编码规范。使用静态代码扫描工具，其结果数据通过质量门限进行控制。云产品、云服务在发布前，均需完成静态代码扫描的告警清零。
- 引入的开源软件遵循开源管控要求，完成开源协议合规、开源漏洞扫描，并满足开源合规执行规则。

持续集成：

- 基于 Jenkins 的代码构建服务，提供灵活的构建资源。支持如：Java、NodeJS、Go 等多种主流语言，以及 Linux、Windows、MacOS 多种编译环境。

测试反馈：

- 测试、研发人员可协同参与测试用例的编写，确保测试需求的实时同步。
- 服务发布前经过多轮安全测试、渗透测试，安全团队通过漏洞管理系统跟踪漏洞修复。

制品库：

- 代码编译后，支持将二进制构建产物推送至如：OSS、S3 等主流云存储，或生成镜像推送至如：ACR 等镜像仓库，便于制品包的快速取用部署。

9 安全运维&运营

面向资产的安全风险管理是乐橙云核心安全管理体系框架之一。

- 考虑到云上资产数量庞大、变化频率快的特征，乐橙云建立了自动化资产管理系统，定期更新云上资产。
- 依据 NIST SP 800-37、ENISA 云安全风险评估、ISO 31000、GB/T 20984 等国际国内标准，制定网络安全风险评估标准，并通过识别、分析、处置、监控环节持续治理风险项。

乐橙云运维团队负责业务的部署、扩容、变更、监控等操作，运维过程需遵守安全运维规范和安全运维基线。

9.1 特权账号管理

日常业务活动不允许使用特权账号，运维人员使用运维账号接入乐橙云管理平面，根据人员职责进行权限分配。

- 特权账号仅在密码和 MFA 验证码均验证成功后启用，密码和 MFA 由不同人员保管。
- 通过 VPN 隧道连接至内网，完成 AD 域认证后，方可进入管理平面。
- 运维账号与员工 ID 一一绑定，使用双因子认证。
- 通过独立的安全团队定期审计，检验账号的必要性和权限的合理性。

9.2 操作安全管理

运维通过堡垒机统一管理云主机、登陆密钥，避免密码、密钥泄露。堡垒机登录强制开启双因子认证。人员操作都有录屏，便于事后审计。

9.2.1 容量管理

在对容量进行监控、预测与规划时，考虑如下几个方面：

- 根据 SLA、业务备份和恢复要求以及容量监控、业务预测结果，制定资源服务对象的监测范围和指标，以及监测周期、阈值、方法和技术等。
- 根据容量监测数据，进行容量分析，分析现有容量与当前服务级别协议和预计要求之间的差距，并提出改进建议。
- 对信息系统进行持续的容量监控，一旦发现异常会及时预警，并实现动态调整和管理。

9.2.2 变更管理

变更操作遵循统一流程化管理要求，通过变更前测试保证变更过程不影响业务的稳定性和连续性。变更流程负责人定期分析变更质量，并对失败变更进行分析评估，定期对流程进行回顾、优化，回顾内容包括关键衡量指标、流程执行效率和流程支持工具的有效性等内容，确保对变更管理流程的持续改进。

9.2.3 威胁防御

安全扫描：

- 定期执行安全扫描，包括 WEB 站点漏洞扫描、应用和服务漏洞扫描、主机漏洞扫描等。

漏洞管理：

- 通过内部安全活动和外部安全研究者反馈，及时发现网站或业务系统的漏洞，并统一管理安全漏洞。
- 安全专员全程跟进漏洞的识别、分析、分配、跟踪、验证直至漏洞关闭。
- 漏洞管理遵守应急响应 SLA 要求。

补丁管理：

- 运维人员遵循《系统补丁管理制度》，规范化补丁更新周期、时间点、测试、操作、备份及回滚，确保补丁的及时、有效升级。

9.3 安全日志及事件管理

9.3.1 日志分析与告警

乐橙云使用 ELK 技术构建了 SIEM 系统，对业务日志、系统日志、安全日志进行收集、关联、分析，制定安全规则自动识别异常事件（包括内部管理系统特权账号的启用，账号创建、修改、删除，账户异地、异常时间段登陆，爆破攻击、网络攻击等），以告警方式通知责任人，通过自动创建电子流程单跟踪问题闭环。乐橙云服务中的安全日志至少保存 180 天，可用于实时查询、审计和事后回溯。

9.3.2 事件管理

乐橙云遵循华橙制定的事件管理流程，对事件实施分级评估。将事件分为特别重大、重大、较大和一般四个等级。采用保护、检测、响应和恢复的方法论提供技术保障能力，事件处理遵守应急响应 SLA 要求。

9.4业务连续性

为消除关键经营活动出现中断的风险，避免遭受重大故障或灾难，乐橙云通过运维平台对云平台的主机、应用、服务、网络等实施实时监控，结合业务故障的自动化报警流程，通过多服务热切换保障服务不中断。除此之外还组织开展业务连续性计划演练和业务影响分析（BIA），持续改进业务连续性策略和 SLA 指标。

9.4.1 灾难恢复

采用主从数据实时热备份、冗余存储和多地备份的方式，保障业务数据安全可靠，持续可用。并对备份情况进行监控和验证。

同时针对业务系统，多链路备用系统，以实现快速应急切换。

9.4.2 应急预案

内部建立对各类型资产、安全及隐私合规风险的应急方案措施，以《业务连续性管理程序》为依据执行，通过有序、高效地应急处理，确保业务的快速恢复。应急方案包括了事前的预案流程、监控和故障应对手段。事中通过系统监控审查记录，提供足够资料用于事件分析。事后优化处理流程方法和应急预案，提升问题处理、分析和回溯能力。

9.4.3 应急演练

根据重要程度和业务实际情况定期开展数据库异常恢复、云厂商切换、用户数据泄露处置等安全及合规应急演练，为应急响应工作提供技术、能力和经验储备。

10 安全承诺

华橙作为以视频服务为核心的智能物联网服务商和解决方案提供商，始终秉承客户第一的原则，非常重视用户的个人信息安全，并采取一切合理可行的措施保护个人信息安全。力求为客户提供一个更安全健康的乐橙云环境。

华橙非常重视网络安全和隐私保护，为此持续投入专项资金，全面提升安全意识与能力，为产品提供充分的安全保障。华橙内部建立了专业的安全团队，为产品的设计、开发、测试、生产、销售与维护提供了全生命周期的安全赋能与管控。华橙产品在坚持数据最小化、服务最小化、严禁后门植入、去除非必要不安全服务的同时，不断引入创新的安全技术，努力提升与完善产品的安全保障能力，更好地满足用户不同场景的安全需求。

华橙成立了网络安全响应中心ISRC（Imou Security Response Center），旨在解决网络安全问题，为全球客户提供可靠、安全的解决方案，包括提供安全通告和预警、漏洞上报和响应流程，分享安全建议和研究成果等。