2019 年 8 月

机智云 IoT 平台安全白皮书

V 2.0

机智云
Gizwits

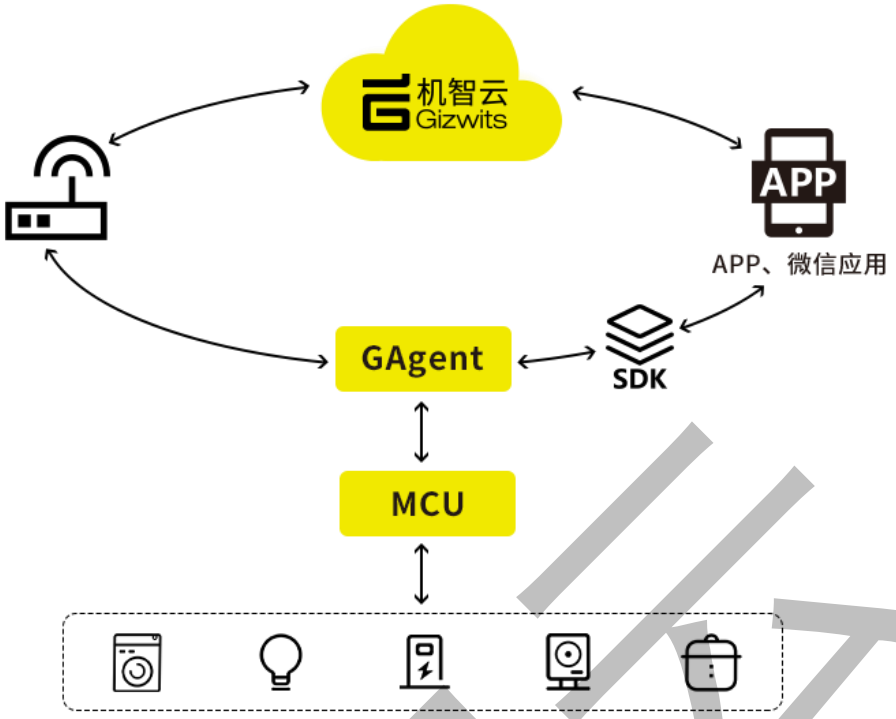
目录

1. 机智云介绍

1.1. 云平台介绍

机智云云平台在全球部署云服务，全球有三大云服务中心，包括国内云、美东云和欧洲云，为全球客户提供安全、稳定可靠、快速的云服务，平台支持异构网络、多协议、多平台设备接入，机智云拥有亿级连接百万并发（单机）的处理能力，能够提供 99.95%服务可用性的不间断服务。

平台提供了从定义产品、设备端开发调试、应用开发、产测、云端开发、运营管理、数据服务等覆盖智能硬件接入到运营管理全生命周期服务的能力。为开发者和厂商提供了自助式智能硬件开发工具与开放的云端服务。通过傻瓜化的自助工具、完善的 SDK 与 API 服务能力最大限度降低了物联网硬件开发的技术门槛，降低研发成本，提升产品投产速度，帮助开发者和厂商进行硬件智能化升级，更好的连接、服务最终消费者。



平台保持与各内外安全权威机构的合作和安全应用落地和演进，同时平台也保持着服务能力和技术的革新升级，机智云 5.0 给开发者和厂商提供了物联网协助应用开发平台，帮忙开发者和厂商快速落地行业应用和解决方案。机智云 C-AEP(协同应用开发平台)是机智云针对物联网行业属性打造的中台架构，C-AEP 包括技术中台、业务中台和数据中台。

技术中台提供物联网端到端技术框架和便捷化工具集合，包括连接中台、APP 框架、产测工具等；

业务中台对物联网设备、用户的通用业务提炼形成服务，供有物联网属性的各类应用使用，快速上线新业务，以达到快速物联网化和满足日益变化的业务诉求；

数据中台对物联网数据进行标准化建模，设备数据、业务数据上传到云端后经过数据治理存储在数据中台的主题库中，包括用户中台、设备中台、应用中台等。

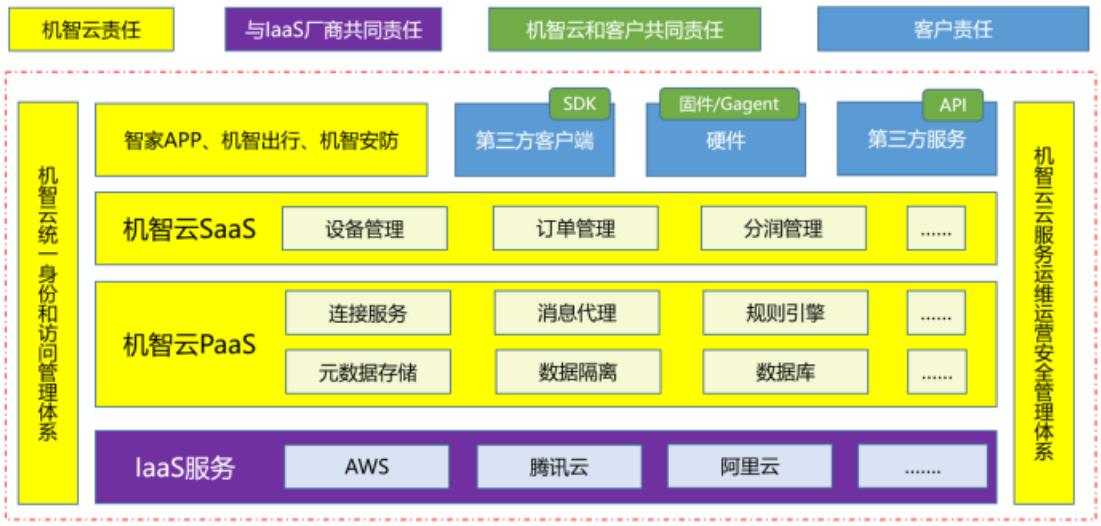
1.2. 信息安全保障的使命

机智云为客户提供安全可靠和符合法规要求的设备接入服务(GDCS)和行业 SAAS 服务，全力保障客户及其用户的数据的可用性、机密性和完整性。机智云承诺：数据保护、数据安全高于一切，机智云在提供稳定可用的服务时，会不断构建完善的云平台安全保障体系，将信息安全保障作为机智云的重要发展战略之一。

为了达成目标和完成使命，机智云严格执行全过程防护机制，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、事后的全过程防护网。

1.3. 安全责任

机智云负责机智云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)接入机智云云需要客户自己保障其应用及数据，包括硬件和 app 的安全合规。下图为基础云服务商、机智云以及客户信息安全责任共同承担责任划分如下所示：



1.3.1. 机智云的安全责任

机智云与全球知名的云主机服务商亚马逊、微软云、腾讯云、阿里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。比如云服务商腾讯云和亚马逊云的安全能力和责任详见:《腾讯云安全白皮书》、《AWS 安全性概述》等等

机智云安全覆盖数据安全和云服务安全。机智云承诺利用安全团队和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，切实保护机智云的安全运营，以及保障客户、用户隐私和数据的安全。包括但不限于如下：

- 数据安全：包括数据分级、数据访问控制、数据脱敏等等；
- 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、接口的设计和开发安全规范、发布、使用等方面。

1.3.2. 客户的安全责任

客户在使用机智云的解决方案的时候，需要严格按照机智云的安全规范和接入要求执行。同时客户需要保证自己的产品和应用的安全性，包括业务后台、客户端、硬件产品安全设计。基于机智云 Gagent 二次开发的固件、SDK 和机智云 APP 框架开发的 APP，机智云仅提供技术支持，但是无法提供任何安全保障。对于基于机智云智家公版的 APP(无任何功能微定制)的数据安全合规、隐私政策等相关信息，机智云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，涉及相关的安全解决方案，基于双方沟通共识，机智云可以提供方案参考和咨询服务。

2. 安全体系

2.1. 数据安全

数据保护是当今企业、政府和个人的基本要求，机智云深刻理解数据安全对客户业务、客户隐私的重要意义，从数据的安全生命周期角度出发，通过对数据产生、数据存储、数据传输、数据使用、数据消亡等各个生命周期阶段制定对应的数据安全管理政策，保证端到端的数据安全。

2.1.1. 数据所有权

使用机智云提供的服务所产生的所有数据归属于客户，机智云是数据的处理者，在符合法律法规、《隐私政策》的基础上，机智云在获得客户和用户授权的情况下可帮助客户和用户保障数据的私密性、完整性、安全性。

2.1.2. 数据分级

机智云对所有用户和企业客户的数据提供安全保护。根据存储和使用的数据实施数据等级保护策略，并按照数据价值和敏感程度对数据等级划分。根据数据安全的分级有对应相应的保护策略和要求，以保护用户和企业数据的安全存储。

2.1.3. 数据访问控制

机智云为企业和用户的数据访问提供安全保障。所有 APP/业务云所使用的数据，严格控制访问权限。任何第三方应用访问和使用企业或用户数据都必须经过企业或用户的授权，同时操作会被记录在相应的操作日志，以便后续追溯、审计使用。

2.1.4. 数据脱敏

为避免敏感数据泄露，机智云对用户和设备的敏感数据进行脱敏和加密保存，实现安全存储，避免被攻击者通过静态分析固件/登录设备后获取文档等形式获取敏感信息。

2.1.5. 数据销毁

用户/企业客户有权限通过 APP/业务后台删除归属当前用户/企业客户的敏感数据，也可以联系官网客服提交删除申请，经过身份验证核对后按流程执行，一经执行数据将无法找回。机智云用于存储客户信息的内存和磁盘需要更换时也会先做逻辑擦除和物理擦除，再交由云服务提供商按行业标准做法对存储介质进行消磁处理。

2.2. 应用安全

2.2.1. 云平台安全

2.2.1.1. 设备身份认证

物联网安全的重点是在设备硬件端，机智云针对不同安全等级的硬件设备提供相对应的设备身份认证方案，以满足不同设备厂商的实际业务需要。

■ 预授权认证模式

对于普通安全等级的设备或者说对成本有严格控制需求的企业，机智云提供预授权认证模式来保护企业设备的身份安全。预授权有以下几种形式：

在设备的产测环节，烧录由云端生成的预授权密钥去唯一标识设备的合法性，设备在上电注册流程必须根据预授权密钥完成注册流程，获取云端生成的设备唯一编号，产测环节的工具是需要经过授权才会提供给企业使用。

厂家提供能够唯一标识通讯设备的编码，如 Wi-Fi 模组的 MAC 地址，或者蜂窝类模组的 IMEI 号，通过机智云的开发者中心或者 API 将这些编码在设备接入云端前提供给机智云。

■ 非对称认证模式

对于高安全等级的设备或者说硬件计算能力较强的模组如安卓、Linux 等设备，机智云提供基于 RSA1024 或 2048 位非对称认证模式。对于一些有特殊需求的客户，机智云还可以支持私有的加密算法的实现。

2.2.1.2. 用户身份认证

■ 机智云平台有以下几类用户：

➢ 接入商用户

接入机智云物联网平台的企业，是以开发者的身份去研发、生产设备，需要对设备进行研发、调试、产测，并且提供售后服务。

- 运营商用户

使用接入机智云的设备，以及配套的业务系统，完成诸如售后服务、共享租赁、设备管理等不同类型的业务。

- 消费者用户

是设备的实际购买者与拥有者;或者在共享业务场景下,是设备的使用者。

■ 针对不同类型的用户，机智云平台提供了不同的身份认证方式：

- 接入商用户

接入商主要使用的是机智云的开发者中心,机智云提供了个人账号和企业账号两种级别，并且每个级别都有所有者、管理者和观察者等多种权限。关键数据只有所有者才可以获取，做到了账号、权限两级的数据保密。同时，个人账号可以加入企业账号，提供了很高的产品使用灵活性。

- 运营商用户

运营商主要使用的是基于机智云 C-AEP 开发的各类业务系统，机智云平台通过企业 API、SNoti、实时大数据、聚合数据、规则引擎等接口向这些业务系统提供必要的功能和数据。机智云通过基于访问密钥的方式对业务系统进行鉴权，并且通过白名单的方式进一步保障安全。

运营商的系统对接机智云平台的时候，对于数据的访问权限受到严格管控，不属于该运营商的数据是不具有可见性的。并且，运营商对数据的关键操作，都会有详尽的记录提供做审计用途。

- 消费者用户

消费者用户身份必须经过注册，提供邮箱、手机号码、第三方系统账号方式，有严格的口令策略保护用户身份不被随意猜测。提供随机短信、邮件激活方式确认用户的真实性。用户必须成功登录后才允许进行业务操作。

机智云平台提供了 OAuth/OAuth2 的能力，可以与第三方的 OAuth ID 提供方集成，很好地对类似微信公众号、小程序，以及亚马逊、谷歌、阿里、百度、小米、IFTTT 等各大第三方平台进行对接。

2.2.1.3. 设备与用户身份匹配

机智云物联网平台为多个不同企业的设备与消费者提供物联网接入服务，设备与用户身份的匹配至关重要。

用户操作设备：必须是有权操作某个设备的用户，机智云平台才允许该用户操作设备。必须是成功绑定或者被分享绑定权的用户才可以控制设备。

设备数据转发至匹配用户：系统具备将设备的状态、数据转发到对应的绑定用户手机应用。

2.2.1.4. 应用层限流控制

应用层的访问控制是物联网平台必须具备的能力，防止接入企业的业务逻辑问题或其他行为导致对平台其他用户的影响。

设备上报频率控制：可对每个产品设备进行上报频率控制，限制不合理的请求额度；

API 时间维度配额访问控制：提供时间段维度总访问额度的控制机制，防止短时间内的高频业务请求；

IP 配额访问控制：提供 IP 维度的访问额度控制；

消费端应用配额访问控制：提供对某个应用的访问额度控制；

单个消费端用户配额访问控制：提供对某个用户的访问控制能力。

2.2.1.5. Web 系统应用安全控制

Web 漏洞控制机制在对外 Web 系统中内置，在技术架构中实现：

SQL 注入控制：WEB 系统框架控制 SQL 注入

跨站脚本：跨站脚本攻击防范

脚本文件上传：严格控制上传路径，文件类型，防止攻击者上传恶意代码，获取主机控制权

2.2.1.6. 传输安全

机智云默认采用 TLS1.2 为设备、应用提供加密传输服务，以确保信息在网络传输中的安全。

对于普通安全级别设备，部分模组从成本角度考虑，无法使用 TLS1.2，机智云默认提供 AES128 位对称加密（或其他加密算法）保护设备端到云端

的传输安全，防止数据泄密。AES 加密（或其他加密算法）在业务层面机智云提供了密钥的动态更新机制，弥补对称加密的不足。

2.2.2. 设备端安全

2.2.2.1. 程序代码安全

设备和通讯模组的代码全部使用 C 语言编写，生产用文件则使用编译好的 bin 文件或者 hex 文件，100%的避免源码泄漏。

产品开发过程，遵守严格的开发流程，包含代码规范管理，代码审核机制，严格的质量测试过程，并使用 Git 进行代码仓库管理，避免因代码开发导致的产品安全问题。

设备日志的信息，需要分级打印，敏感信息（比如设备的 ID，静态密码等），使用星号代替，避免因调试信息导致的信息泄漏。

2.2.2.2. 数据储存安全

设备的云端注册、预处理过程，全部使用 AES 128 位加密算法进行数据加密，保证数据内容的安全性。

设备静态敏感数据，包括设备的型号密码、设备本地访问密码、设备预授权密码、设备 ID 号经过混淆加密后保存到设备的 flash 中。

设备存储到 flash 的离线日志，是经过混淆压缩后的日志编码，无任何明文日志信息，保证了离线日志的安全性。

设备支持云端下发的重启、重置命令，可以根据产品需要进行远程操作，必要时，可以销毁设备上的所有数据。

2.2.2.3. 设备防伪

机智云支持多种预授权处理，设备在注册到云端前，必须获取到合法的授权密钥才能正确的进行云端注册，杜绝了非法设备的连接。

授权密钥支持生产时烧录，即一机一码，杜绝设备盗用预授权密钥。

为防止模组被固件被不正当使用，并验证模组固件真伪，需要模组启动后进行身份验证：

- 模组启动后，需要从 flash 读取生产数据，并提取身份验证数据，首先对整体生产数据进行 hash 校验，确保身份验证信息正确，然后通过模组的版本号、mac、以及验证信息中的加密因子结合，计算出身份校验 ID，最后和 flash 中的验证信息里的身份 ID 比对，一致则通过，不一致则重启。

2.2.2.4. 支持标准 TLS 以及自定义的传输加密

模组支持 TLS1.2 的链接层加密，也支持 AES128 位的数据层加密。

模组支持透传模式，在此模式下，设备可以使用自定义的数据加密算法对设备进行加密传输，此时，模组作为数据通道，在 TLS 的加密链接下，对数据做双向转发，设备和上层应用负责数据层的加密和解密。

2.2.2.5. 配网安全

机智云支持 softap 和 airlink 两种方式配网，配网内容经过 AES 加密后传输，保证配网的安全性。

机智云支持蓝牙配网，手机和设备蓝牙点到点数据通讯，并且配网内容经过 AES 加密，保证配网安全性。

2.2.2.6. OTA 安全

OTA 细分为模组 OTA 和 MCU OTA，避免 OTA 混淆带来的固件升级失败问题。

OTA 的请求过程使用 AES 进行数据加密，保证了数据安全性。

OTA 的文件中使用 md5 进行文件校验，避免了设备升级了错误或者不完整的文件带来的启动异常的问题。

OTA 固件中去除敏感信息，纯粹二进制文件，防止出现设备 OTA 文件外泄导致的信息丢失问题。

OTA 过程支持断点续传，最大程度的保证设备 OTA 的成功率，避免设备长时间处于 OTA 失败的过程引发的安全问题。

支持推送 OTA 和上电检查 OTA 两种方式，第一时间响应 OTA 请求，加快 OTA 的过程。

2.2.3. 移动应用安全

2.2.3.1. 存储安全

存储安全是应用安全中非常重要的一环。

- 在 iOS 中，机智云对需要本地存储的敏感数据（Token 等）保存在”Keychain”中，在存储过程中，使用了两个不同的 AES-256-GCM 表加密元数据和密匙，确保了敏感数据的安全。

- 在 Android 中，机智云使用”Keystore”来确保数据的安全。Keystore 可以保护密钥在信任的环境下使用。Keystore 可以防止外部从进程和设备中获取密钥，避免了以未经授权的方式获取和使用密钥。

2.2.3.2. 网络通讯安全

- 机智云移动应用符合 App Transport Security(ATS)安全机制，确保安全的网络通讯。

2.2.3.3. 应用热更新安全

- md5 校验 OTA 包的完整性
- 创建应用的时候生成密钥，分别存储在云和 App，用于 OTA 更新时校验 OTA 包的合法性，防止恶意推送更新。

2.2.3.4. 应用唯一性

- 应用启动会执行完整性校验，确保应用没有被篡改、二次打包。

2.2.3.5. 代码安全

- 机智云采用独特的加壳保护，保护 App，防止静态逆向。
- 使用防逆向保护，代码插花，代码混淆、代码切片、虚假控制流、字符串加密、控制流平坦化等技术，确保代码的安全。

2.2.3.6. 运行保护

- 为了确保运行时的应用安全，机智云对内存、本地数据和资源文件进行了加密。
- 使用对抗信息窃取和防动态调试技术，防止从外部窃取应用数据。
- 内存防 dump 保护。

2.3. 系统网络安全

2.3.1. 系统安全

机智云与腾讯云和亚马逊云深度合作，由云服务提供商负责整个云计算环境底层的物理和基础架构安全，提供包括漏洞发现、补丁修复、升级更新、审计监控等安全管理措施。机智云也会定期委托第三方安全公司，对操作系统、网络、中间件、应用做相关安全测试，及时整改，确保系统符合相关安全要求。

2.3.2. 访问控制

访问所有承载、存储用户和企业数据的系统时，机智云必须通过堡垒机登陆。高密级数据的访问必须细化到个人，必须有安全的登录机制，所有人的访问已授权且符合最小化原则，所有行为日志记录齐全且远程备份满足可审计。

2.3.3. 网络安全

2.3.3.1. 网络隔离

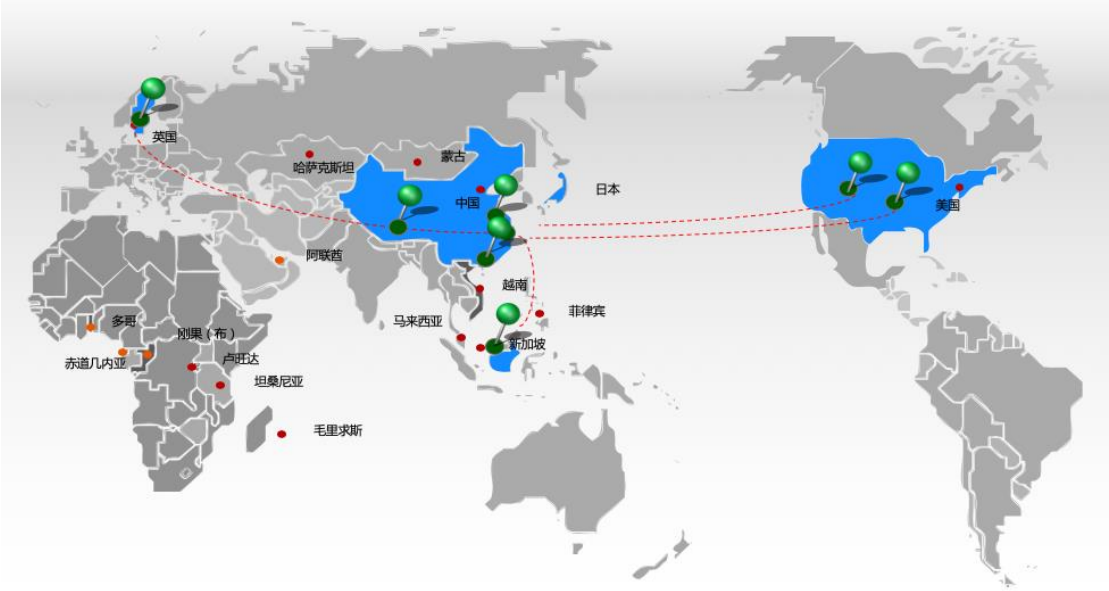
机智云制定了严格的内部网络隔离规则：

1) 办公网络、开发网络、测试网络和生产网络之间物理隔离和逻辑隔离。私有云、专有云和公有云通过虚拟化控制访问策略做网络隔离。

2) 访问权限隔离。非授权人员禁止访问任何内部网络资源，授权人员只能通过 VPN 网络登陆堡垒机后访问相关授权网络。

3) 云端用户按权限划分，访问时需经过身份验证、证书验证、密钥验证或接口 token 验证等安全机制验证后，方可访问当前人员的私有数据。

2.3.3.2. 网络冗余



机智云数据中心遍布全球多个区域，覆盖中国、美国、欧洲、亚太等地，通过云服务商的专线构建了同城多物理机房，异地多数中心的安全网络，具备跨地域的灾备能力，有效地降低运营商公网故障带来的持续性影响，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甚至多云切换的能力。

2.3.3.3. 入侵检测和防护

机智云依托腾讯云、亚马逊云等知名云服务商提供成熟的网络安全架构，实现了全方位的防护，在各个层面均部署了安全防护，包括安全体检（漏洞扫描、挂马检测、网站后门检测、端口安全检测等）、安全防御（DDoS 防护、入侵检测、访问控制来保证数据安全与用户隐私）以及安全监控与审计，形成事前、事中、事后的全过程防护，以应对来自互联网的各种威胁。

2.3.4. 运维规范

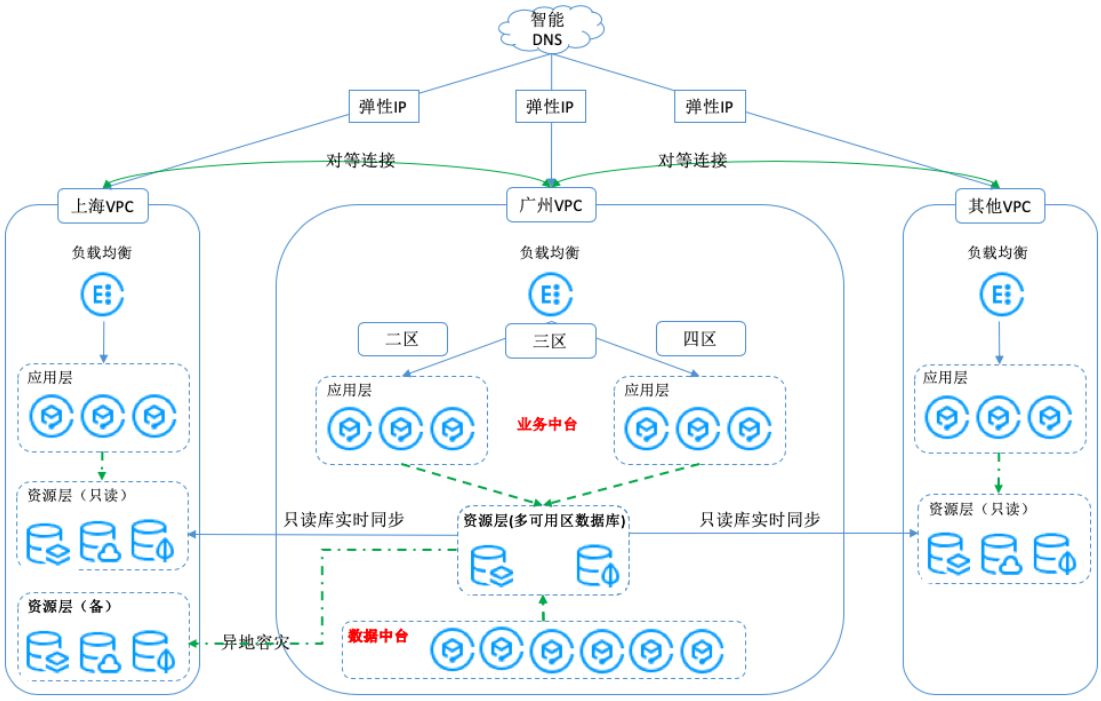
机智云通过严格的内部管理制度，配合自动化、工具化的运维管理平台来确保运维安全。

- **认证**：运维人员必须经过堡垒机方可访问客户数据所在的生产环境，且所有运维账号均配备双因素认证机制。
- **授权**：在授予权限时，通过细颗粒度在权限划分确保只授予员工提供相应服务所需要的最小权限，所有额外授权的申请均需要经过多次的评审和批准。
- **监控**：运维团队实行 7x24 小时应急响应值班机制。一旦发生安全事件，将根据不同事件等级进行响应与处理，与用户客户相关的安全事件将被赋予最高优先级处理。事件的管理包括整个事件的受理、通告、处理、与事后总结整个过程。事件的总结工作会从技术、流程、意识等多维度从根本上进行原因分析，并落实责任惩罚，以防止类似事件的再次发生。

- **审计**：所有漏洞与事件的响应均实现平台化和线上化处理，所有记录完整可查询，任何内部人员在未获得客户的同意与授权时均无法触碰客户的云端业务数据。运维团队会对各类安全数据进行定期汇总和分析，并向公司高层呈现与汇报。

2.4. 容灾和业务可持续性

2.4.1. 云服务多地多活架构



为承诺和保证机智云物联网平台服务的品质，机智云制定和严格执行服务级别协议。为防止业务活动的中断，保护业务流程不会受信息系统重大失效或自然灾害的影响，并确保他们的及时修复，机智云严格执行灾难恢复与业务连续性管理要求，主要包括：

- **备份管理与数据恢复**：机智云上的用户数据在多个系统及多个数据中心进行复制存放，并依据业务要求设置相应的备份程序、频率、保存周期。不同数据中心地理位置呈分布式状态，以达到远程互备的效果。备份介质和恢复程序会定期进行检查和测试；
- **制定和实施业务连续性计划**：机智云通过制定和实施计划来保持或恢复业务的运行，并定期对计划进行测试、维护和再评估，以在关键业务过程中断或失败后能够在要求的水平和时间内确保信息的可用性；
- **灾难恢复演练**：机智云定期进行灾难恢复演练，实施完整的演习，以测试组织、人员、设备、设施和过程能够应付中断。所有的演练情况均会予以记录和总结，并采取措施改进。

2.4.2. 离线业务支持

在设备完全不联网的情况下，机智云设备支持纯小循环控制，这种模型对于某些场景特别适用，比如工厂内网环境，100%杜绝数据外泄。

设备支持热点模式下的直连访问，不需要路由器，手机可以连接设备热点直接操作设备，方便在户外等环境的使用。

设备在连接云端异常时，支持设备日志的存储，以方便后续设备问题的排查。

设备在连接云端异常时，MCU 产生的数据可以保存，且进行压缩处理，当云端回复时，将数据进行及时上报，防止网络问题带来的数据丢失。

3. 安全合规

机智云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、设备端、APP、业务后台等需求实现过程中严格执行。

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

目前，机智云已经通过全球多个代理机构的认证，是一家拥有多个认证的 IoT 解决方案提供商。

3.1. 工业互联网平台可信服务

机智云通过工业互联网平台可信服务评估测评。

工业互联网平台可信服务评测由工业互联网产业联盟组织，聚焦信任，围绕“是否对用户关心的问题都进行了真实的、规范的承诺”设计 24 个指标，通过材料审查、技术测试及现场考察的方式对平台服务进行评测。

工业互联网平台可信服务评测将助力工业互联网平台服务企业建立行业服务公约，让用户放心使用平台，让竞争更有序。

3.2. ISO27001

机智云已通过 ISO27001 认证。

ISO27001 是一项被广泛采用的全球安全标准，采用以风险管理为核心的方法来管理公司和客户信息，并通过定期评估风险和控制措施的有效性来保证体系的持续运行。

ISO27001 为一个系统的、整体规划的信息安全管理体系，其从预防控制的角度出发，保障组织的信息系统与业务之安全与正常运作。ISO27001 体系共分为两部分：信息安全管理实施规则：该部分对信息安全管理给出建议，供负责在组织启动、实施或维护安全的人员使用；信息安全管理体系规范：该部分说明了建立、实施和文件化信息安全管理体系（ISMS）的要求，规定了根据独立组织的需要应实施安全控制的要求。

ISO27001 信息安全管理体系的目标为通过整体规划的信息安全解决方案，来确保企业信息系统和业务的安全，并保持持续正常运作。

ISO27001 认证是关于信息安全管理体系认证，ISO27001 将有效保证企业在信息安全领域的可靠性，降低企业泄密风险，更好的保存核心数据。

3.3. ISO9001

机智云已通过 ISO9001 认证。

ISO9000 质量管理体系是企业发展与成长的根本，ISO9000 不是指一个标准，而是一类标准的统称。ISO9001 质量管理体系是国际标准化组织（ISO）制定的国际标准之一，在全球范围内得到该组织的 100 多个成员国家和地区的认可。ISO 9001 概括了一个面向流程的方法，用于记录和审核在一个组织内实现有效的质量管理所需的结构、责任和规程。

3.4. GDPR

GDPR，全称是 General Data Protection Regulation(通用数据保护条例)，它由欧盟推出，目的在于遏制个人信息被滥用，保护个人隐私。

GDPR 要求从事个人数据处理的所有人必须遵守其规定，并赋予个人数据正在处理的个人一些重要的权利。参与个人数据处理的自然人和法人，包括公司和政府机构，都被要求按照 GDPR 行事。潜在的不合规行为可能导致高额罚金，并导致法院诉讼和名誉损害的后果。

在 GDPR 生效之前，机智云已全面推进数据保护工作。GDPR 许多要求的重心都是确保有效控制和保护个人数据。机智云为客户提供账号删除功能，全球客户可以自助操作销毁相应的个人数据。机智云用于存储欧洲客户数据的所有服务器均位于欧洲--准确的说，是在法兰克福。

3.5. VDE

VDE 标志在世界范围内对于电子产品来说都代表着保护和安全性。VDE 研究所通过对电气产品的整体、中立和自主测试，致力于其安全性、电磁兼容性和操作性能。此外，VDE 研究所为制造商在其产品质量上的投资提供支持服务。

使用机智云服务的部分客户已通过 VDE 的相关认证，机智云所提供的服务符合 VDE 的相关安全规范。