网安卫谷
WEIGUTECH

让安全随手可得

智能移动终端安全管控平台

技术白皮书（通用版 V7.3）

2022 年 9 月 21 日

浙江网安卫谷科技有限公司

版权说明

文档信息

文档密级	保密文档
阅读对象	最终客户、公司内部成员

联系我们

网址：http://www.weigutech.com

邮箱：info@weigutech.com

地址：中国天津市南开区南京路 309 号环球置地广场 34 层

目 录

1.概述

网安卫谷企业移动安全管理平台（Mobile Device Management，简称为 MDM）是针对党政、军工、金融等用户提供移动安全管理整体解决方案，通过终端空间隔离、应用沙箱等技术实现对设备、应用、内容的管控，构建企业信息化安全办公平台，帮助政府企业应对日益严峻的移动互联网安全风险。

本文所述的移动终端指企业员工在企业移动计算环境中使用的便携式电子设备，包括智能手机、平板电脑、智能终端设备等。

本文所述的移动终端安全管理指为政企客户提供的移动终端、应用与数据的全生命周期的安全管理解决方案，主要包括移动终端设备管理，应用管理，合规审计，个性化，平台配置管理，数据仪表，运维管控，口令认证，终端设备等功能。

移动终端安全管理根据部署方式的不同，分为项目型解决方案和平台型 SaaS 服务产品两种。项目型解决方案是在客户侧部署专用移动终端安全管理服务器，为行业大客户提供定制化服务；平台型 SaaS 服务产品是在云端集中部署移动终端安全管理平台，以租赁方式为中小企业和聚类客户提供标准化服务。本方案描述在实施项目型应用时的解决方案，包括需求分析、技术方案、部署方案、商业模式、服务流程及合作伙伴介绍等内容，为解决方案落地实施及营销推广提供依据与指导。

移动终端安全管控解决方案，主要面向对移动设备安全管理要求较高，要求在企业侧部署移动终端安全管理服务器，有定制化需求，对价格相对不敏感的大中型政企客户。目标客户主要为：营销性质企业客户，例如零售、保险、医药、汽车销售等行业客户；信息化程度高的大型企业客户，例如电力、金融、保险、基金、交通物流、生产制造等行业客户。

2.需求分析

随着 5G 时代的到来，企业信息系统移动化应用发展迅速，众多企业通过移动应用

来提高工作效率和客户服务质量，企业员工使用个人移动终端设备进行移动化办公的情况日益增多，智能手机和平板电脑成为了重要的事务处理和通讯平台。

近年来 IT 技术和通讯技术的进一步融合，移动互联网产业得到了迅猛发展，逐渐渗透到人们工作、生活的各个领域。基于 Android 以及 HMS 操作系统的智能终端设备具有普及程度高，计算能力强，存储容量大的特点，利用智能终端设备访问企业 IT 系统进行移动办公成为市场潮流。

新技术的不断发展，移动终端的操作系统也逐渐多样化，如 iOS、Android、HMS、等等，另外终端厂商、终端型号也五花八门，这些现状都对其中存储的企业数据造成一定的风险，一旦发生设备被盗或遗失、恶意软件/病毒感染，将使企业和个人蒙受重大损失。

截至 2021 年，我国的数据安全监管框架已经基本成型：《网络安全法》、《数据安全法》、《个人信息保护法》成为数据安全领域的“三架马车”。此外，在银行、通信、工业、能源等各领域也已经有一系列条例规章从实践角度推动产业内数据安全治理体系的落地，市场亟需解决数据末端计算、存储、使用过种中的合规安全管控工具，来辅助数据安全体系构建企业的数据合规防线。

随着移动信息化的广泛应用以及移动终端的智能化、复杂化发展，对于政企客户，如何对移动终端、应用和数据进行有效的安全管理，已经成为一个愈来愈需要重视的问题。目前大量移动终端正处在一个保护极其脆弱的运行环境中，面临诸多安全漏洞的隐患及侵入风险。同时，政府在数据隐私保护和加密方面的法律法规也越来越严格，甚至会对违规行为加以处罚。另外，基于多种操作系统和移动终端的应用程序开发、整合及管理等工作，大大提高了企业移动终端应用的管理成本。企业如要安全、有效地推进移动信息化发展，就需将控制和保护移动资产的措施落实到位，实施有前瞻性的管理和安全举措，确保在提高工作效率、提升客户服务质量的同时，加强对企业移动终端和数据信息的管理和保护，同时通过规范企业终端用户的使用行为，切实保护移动终端、应用

和数据的安全。

政企客户对于移动终端安全管理具体需求将通过以下几个章节描述。

2.1. 数据合规防护需求

进入 2022 年，与数据安全相关的政策还在继续细化。国家互联网信息办公室颁布《网络安全审查办法》修订版，将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查。然后,国家九部委联合发文规范平台企业发展，再次针对互联网企业合规经营，强调防止数据过度采集、打击黑市数据交易、大数据杀熟等滥用行为。在严格保护算法等商业秘密的前提下，支持第三方机构开展算法评估，引导平台企业提升算法透明度与可解释性，促进算法公平。要求平台企业深入落实网络安全等级保护制度，探索开展数据安全风险态势监测通报,建立应急处理机制。

2022 年 2 月 10 日，工信部发布通知,再次公开征求对《工业和信息化领域数据安全管理办法(试行)》的意见。可见，与数据安全相关的管理办法等细则正在加速落地。

综上我们可以看到，在新的数据安全监管体系下，我们看到数据安全正在从传统的“系统视角”(保护存放数据的系统设备)向“业务视角”(围绕数据流动展开全生命周期防护)转变。以数据与算法为核心的监管正在深刻影响国内 IT 产业格局。数据和算法安全已经成为互联网乃至所有数字化企业的监管核心内容，也将对其盈利能力、商业模式、成长边界等将产生深远影响。

未来，所有企业为满足数据安全的合规要求将进行越来越多的投入，尤其是游离于内部安全网络之外的移动终端，在移动化、物联网的时代背景之下更需要解决数据安全合规防护的相关问题，确保用户体验与安全诉求平衡发展，推动国家数字经济规划再创新高。

2.2. 企业资产审计管理需求

企业员工使用智能手机、平板电脑等移动终端无线访问企业资源的工作方式有效地

提升了员工工作效率，节约了企业成本，提升了企业管理水平，得到企业的广泛认可。

然而，对于企业移动终端设备的管理，很大程度上区别于传统意义上对企业拥有的设备资产的管理，尤其是在区分企业、个人所拥有的设备和数据问题上，需要在充分考虑保障隐私的前提下，对移动终端、应用和数据进行有效的安全管理。

企业 IT 部门需要实现对企业移动终端用户及设备的管理，具体包括对企业内各部门、各员工及其名下移动终端的资产管理、日志管理、统计分析等功能。对企业移动终端实现注册、分组、停用、注销等可控性操作，例如对离职员工手机终端中存储的企业应用及数据进行删除。另外，要求能够对移动终端的基本信息和运行状况进行了解，例如当发生一些违规操作时，如用户终端进行越狱、Root 等不安全操作，或者用户违规更换设备时，企业客户的 IT 管理部门要求能够收到及时的告警提醒，以及进行相应的管理操作，从而确保企业信息的安全。

2.3. 终端硬件管理需求

移动环境和一线工作环境复杂多样、管理不便，对 IT 部门来说，要想积极主动而有效地管理企业所有设备、应用程序、数据等是极具挑战性的工作。企业需要在保障员工使用工作所需的企业应用和数据的前提下，为 IT 部门针对终端设备、应用和数据提供集中、便捷的管理和保护手段。企业设备硬件管理需求，主要包括为企业各级管理人员、一线工作人员提供方便的管理服务，例如对终端的摄像头的开关进行配置等，从而实现复杂移动环境和一线工作环境下，对企业移动终端设备的硬件管控。

2.4. 终端配置策略管理需求

对企业内移动终端进行安全管理和防护，监控企业内移动终端的总体安全状况，并进行安全策略配置管理，包括终端安全参数采集、安全事件采集与分析、终端安全策略配置与实施等，以确保企业内移动终端及其应用与数据的安全，具体措施包括统一的开机密码设置、移动终端的数据加密、移动终端丢失后的远程锁屏、远程数据擦除、违规

设备的隔离与恢复、对移动终端进行定位、定期对移动终端的应用和数据进行备份并且随时进行恢复等。要求管理员能够批量推送部署证书，对证书进行有效的管理。实现对企业移动终端进行远程配置管理，比如提供邮箱、WIFI、VPN 等远程、批量配置，以及终端密码管理策略，比如密码长度、复杂度、密码有效期等的策略配置等。

2.5. 终端应用及数据管理需求

应用个人移动设备进行移动办公将使得商务办公和私人活动的界限越来越模糊，这种趋势直接导致了企业在管理移动设备的安全及避免重要数据外泄方面面临着更大的困难和挑战。

企业要求实现对企业移动应用的发布、远程推送与分发、批量部署的管控，并且能够针对不同部门、用户，提供不同应用的部署。以及实现对企业应用安装、更新、卸载及使用情况的监视与管控，以及对终端上应用的合规性进行检查等。并能够实现对企业数据进行安全保护管理功能，例如数据备份与恢复、数据全部/部分擦除、数据加密、数据防泄露等功能。

2.6. 智能手机的个性化定制需求

- 手机支持通话加密，防止被第三方以其他手段进行窃听。
- 防止人员通过 ROOT、刷机、换卡、换非定制的智能手机、恢复出厂设置等手段脱离管控或泄密行为。
- 预置唯一的安全应用商店，且限制只能从这个应用商店下载安装移动应用，规范手机软件管理，抵制恶意软件入侵。
- 手机外观、开关机画面、壁纸等方面要体现组织文化的特色。

2.7. 上网行为的管控需求

- 能够提供谁什么时候访问了哪个网站的审计能力。
- 能够按平时或者节假日、按用户组设置不同的上网时段对上网行为进行时间管控。

- 能够提供网站白名单管理，仅允许访问白名单中允许的网站，其他网站都应该被禁止访问。
- 能够对网页内容和标题、搜索引擎进行关键字过滤，避免成员搜索不健康的网站和打开不健康的网页。

3.国内外同类产品技术发展状况分析

国际主流厂商包括：IBM、VMware（AirWatch）、BlackBerry、MobileIron 等，利用终端设备管控技术构建 UEM（unified endpoint management）作为下一代移动安全管控产品演进路线。UEM 近几年主要用于管控企业的移动及桌面终端，未来将加入对可穿戴设备和物联网（IoT）设备的支持。

根据 Gartner 预测分析，随着新设备和更复杂的界面出现，企业 IT 部门将面临着向统一终端管理策略的压力，该策略允许在一个界面下管理所有企业设备。企业未来将不得不在几年内升级原来的 MDM/EMM 产品到 UEM，来解决未来即将进行的企业物联网（EoT）的部署工作。

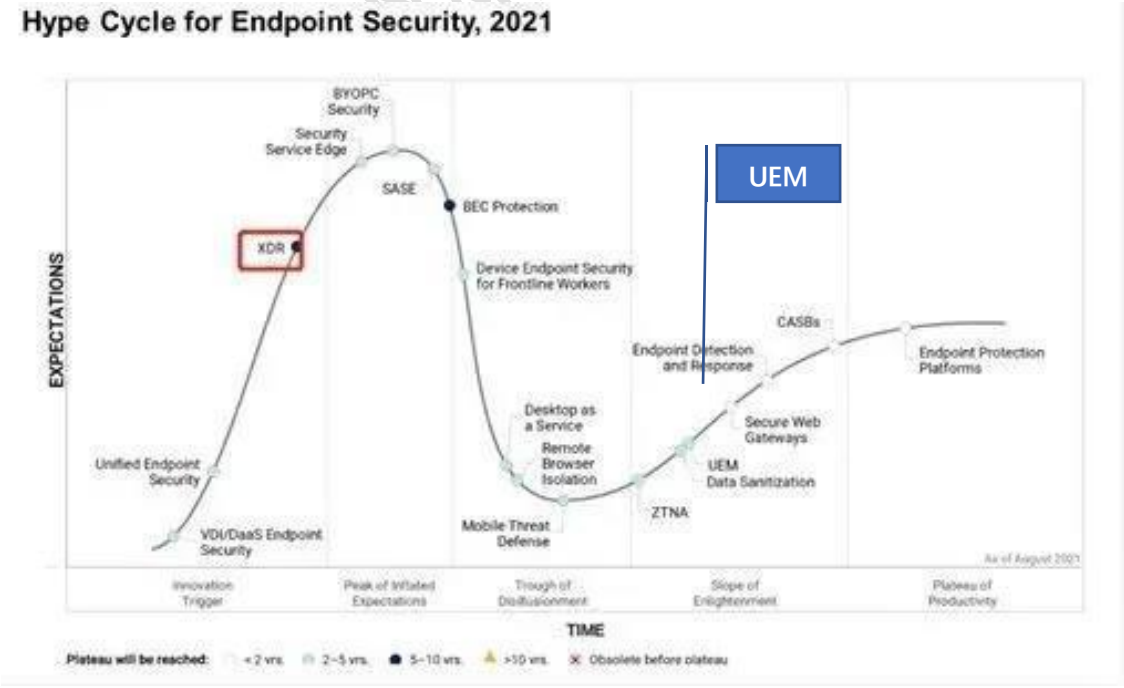


图 3-1：2021 年端点安全技术成熟度预测

实际应用中，许多中大型企业 CISO 为应对日益复杂的网络攻击，往往会采用大量

不同厂商的安全设备。据 2020 年 Gartner 发表的 CISO 使用情况调查报告可知：78%的 CISO 同时使用超过 16 种来自不同安全厂商的安全产品，12%的 CISO 会同时使用超过 46 个安全产品。这将直接导致运维成本增加，效果却甚微。

Unified endpoint management（UEM）通过以员工为中心的运行 PC 端、移动端的端点设备视图，为计算机和移动设备提供基于有代理和无代理的管理，其强调通过整合不同的安全工具并简化跨设备和跨操作系统的流程来简化端点管理。

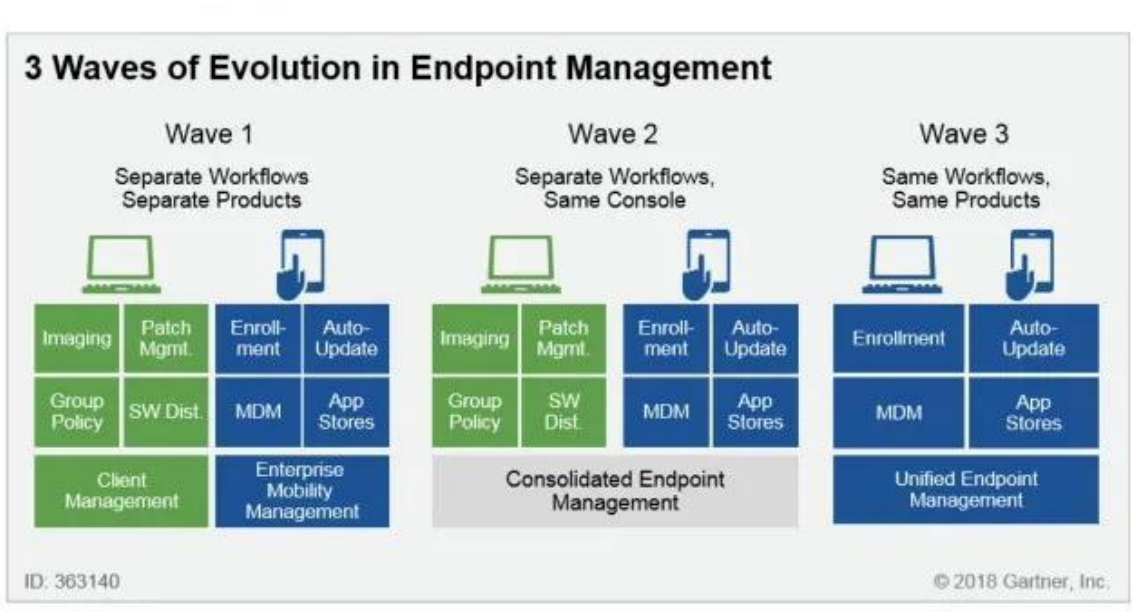
远程办公的流行，企业需要支持用户拥有的任何设备能快速访问业务，这导致了使用多个系统的安全挑战。继 2020 年，Gartner 首次在端点安全技术成熟曲线中提出 UES 后，2021 年继续将 UES 的最新概念纳入炒作周期。

Unified endpoint security（UES）将端点保护平台（EPP）、威胁检测与响应（EDR）、移动威胁防御（MTD）功能单一的控制台整合到一个统一的平台下，从而提供更好的安全概况和更简单的管理。采用 UES 企业将获得俩点好处：

（1）将传统 PC 的威胁预防、检测、事件响应能力扩展到移动设备。

（2）在单个控制台即可统一端点安全和管理工作流。

随着党政头部客户安全建设的成熟，未来能够提供一体化解决方案的厂商更受青睐。UEM 与 UES 的融合发展，将是端点安全厂商的新方向。



Source: Gartner (June 2018)

图 3-2：MDM 发展阶段

目前来看，国内 UEM 的厂商非常少。一方面国内基于 PC 和移动端的原生应用程序还存在比较大的体量，转型需要时间，另一方面国内企业对 PC 端的管控要求非常复杂，很多原生的 API 不足以满足管控要求，同时大部分客户还希望对混合接入的 IoT 终端进行统一管理，绝大多数 EMM 厂商不具备 PC 终端和 IoT 终端的管控能力，导致国内 EMM 厂商往 UEM 转型的非常少。所以国内 UEM 厂商一般都是由少数同时具有 EPP 和 EMM 产品的厂商来落地。

近几年随着国内网络安全法、数据安全法和个人信息保护法相继落地，三部法律形成了一张强大的安全保护网来保护公民个人信息的安全，也保护着国家数据的安全，成为建立社会主义数字化强国的坚强后盾。对于移动设备的安全管控需求，无论是以上三部法律还是基于三法形成的各行各业的法规、条例、条令、办法、标准规范等，都进一步要求对移动设备的通信、身份、接入、应用、数据等进行全方位安全升级。

国内各个厂商，如启迪国信、指掌易、嘉赛、慢吉等，也相继从单一 MDM/EMM 产品线转战“零信任”市场，纷纷投入相关“安全网关、物联终端、大数据安全分析”等方面研发，预计未来几年国内市场 MDM 单一产线的厂商会逐渐消失，被综合安全厂商所兼并或替代。但 MDM/EMM 的关键技术并不会消失，反而会根据国内对于国产操作系统的热衷需求，迎来全面的新突破，与国际技术路线出现路径不同但目标一致的现象，即安全的“殊途同归”。

4.网安移动安全管控平台市场前景

2021 年 8 月 20 日，我国发布了《中华人民共和国个人信息保护法》，确立了确立个人信息保护原则以及禁止大数据杀熟等现象，进一步完善了我国个人信息保护，肃清网络环境。从我国“十四五”规划内容可以看出，我国从基础设施建设、保障体系构建、人才培养、宣传教育、全球合作等方面进行网络安全行业的布局与发展，将网络安全提

升到战略新兴产业的高度。另外，以滴滴上市叫停事件为导火索，国家对于网络安全的重视程度可见一斑。未来，我国网络安全行业的市场规模将进一步扩大，预计到 2026 年，市场规模将逼近 4000 亿元大关。

图 4-1：2021~2026 网络安全行业市场规模预测

2016 年至 2024 年期间，全球企业移动安全市场以 19.4%的年复合增长率增长。2021 年，全球企业移动安全市场规模达到 43 亿美元。2021 年，全球企业移动安全市场占比很小，只有 1.06%。

目前中国企业级移动安全市场规模预计在 20～30 亿元之间，未来市场容量预测约 60 亿元。未来随着国家加强对移动应用隐私保护与合规监管，移动安全市场投资增长潜力较大。移动安全厂商更倾向于产品标准化而非定制化，在统一标准、统一产品，为客户提供多种标准服务的基础上形成商业发展模式。未来移动安全市场的发展一定是紧密和业务应用结合，走平台化战略。

我国当前数据安全市场规模达数十亿元。根据计世资讯数据 2018-2021 年平均年增长率约 31.8%，如按照 31.8%增速计算，2021 年中国数据安全市场规模 69 亿+人民币。随着《数据安全法》的出台以及滴滴事件的催化，数据安全在今年成为网络安全行业关注度最高的细分方向之一，政企用户在数据分级、数据治理，以及数据全流程管

理、数据保护体系的建设预计将成为安全支出的重点，包括在金融、政府等关键部门，以及电信、能源、医疗等行业都有着迫切的数据安 全建设需求。

网安自 2016 年就奠定了移动安全行业移动终端安全管控平台软件产品的市场地位，服务了多个国内政企大客户，并以此产品为基础升级研发 EMM 企业移动管理安全平台产品，该 EMM 产品能力包括 MDM 移动设备管理、MAM 移动应用管理、MCM 移动内容管理三大子系统，客户覆盖金融、工业、军营、政府、司法等多个行业，完美解决政企客户移动办公场景的安全防护问题。

今年公司规划在 EMM 平台基础之上，构建新一代的移动安全与数据安全的融合产品： 网安密+智能移动终端安全管控平台，它将重新定义移动应用安全开发、移动安全办公和移动数据安全防护等业务领域。该产品以移动化属性占领应用安全、数据安全在移动智能终端的细分领域，为用户在移动终端业务场景提供终端、应用、数据安全防护的全方位综合解决方案。

网安移动安全管控平台作为新一代数据安全领域的移动安全产品，横跨移动安全与数据安全领域，是移动安全在数据安全领域的一个细分市场；也是数据安全在移动安全领域最优解决方案；未来该产品将通过公司在移动安全十几年的技术积累和经验沉淀，融合公司近年来在数据安全领域技术的突破，持续创新移动端综合安全防护技术，有效补充数据安全在远程终端的脱机闭环防护手段，拓宽移动安全在工业互联网、智能制造、物联网、车联网等智能终端边缘计算、边缘存储等节点场景的安全防护措施，为我国建设数字中国、网络强国增添一份安全助力，致力于成为中国“数字产业的新一代安全技术基座”！

5.设计方案

5.1. 总体架构

随着移动互联网的飞速发展，国内数字经济迎来新的发展，企业越来越重视移动应

用在企业数字化变革中的积极作用。随着世界新冠疫情的爆发，企业加快了数字化变革的进程，远程办公场景更多地利用移动设备进行身份认证、鉴权以及直接利用 APP 进行内网办公。通过移动终端的特色能力构建零信任的企业数字化安全办公整体架构已经进入技术推广阶段，因此企业需要对移动终端进行灵活且安全的管控系统，来保障移动终端设备自身的安全，从而让其胜任安全办公零信任整体方案中不可或缺的关键作用。

移动终端安全管控平台充分考虑了企业的发展趋势和需求，针对国内政策特点，专属为政企客户提供基于国产品牌智能终端的全生命周期的安全解决方案，帮助政企用户应对终端设备管理、终端应用、终端身份管理、终端行为审计等面临的安全风险，实现政企客户利用移动终端达成安全接入、安全通信、安全认证、安全数据管控等方面的企业数字化安全远程办公的目标。

移动终端安全管控平台整体架构如下图所示：

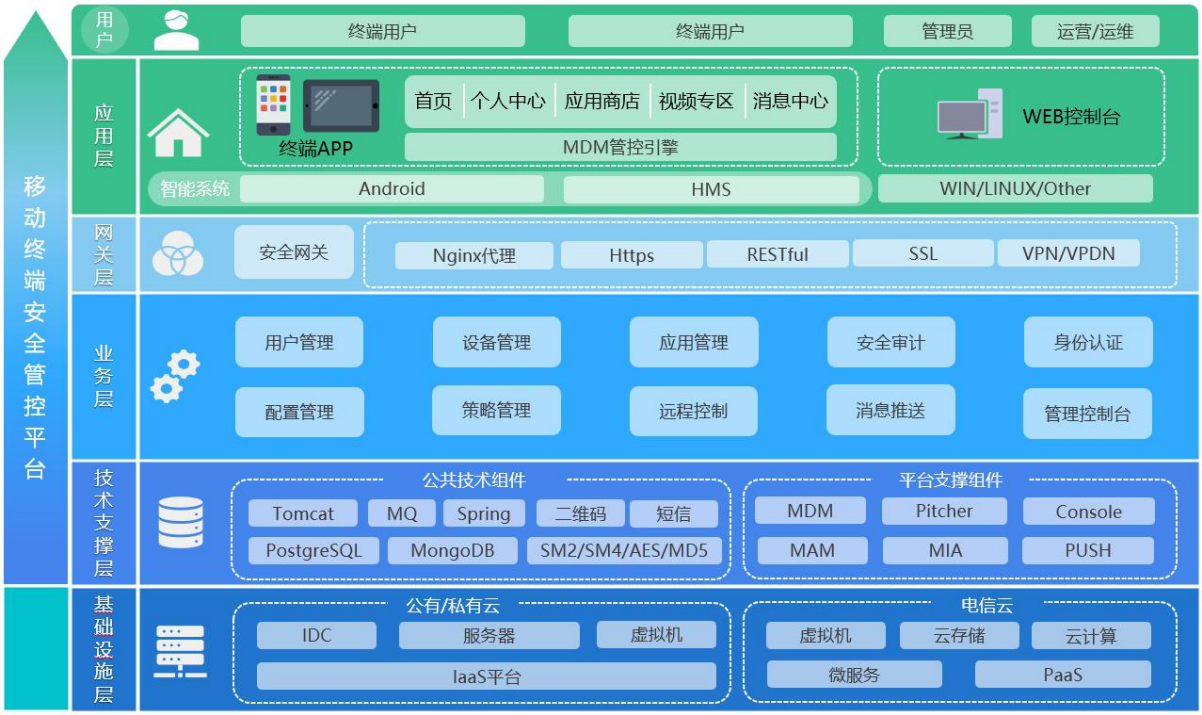


图 4.1：移动终端安全管控平台架构

移动终端安全管控平台整体架构分为五层，分别是应用层、网关层、业务层、支持支撑层和基础设施层，其中前四层为平台主体部分，以应用软件和系统服务的形态体现。而最后一层基础设施层为移动终端安全管控平台服务的承载硬件设施，一般为物理服务

器或云计算服务的虚拟机/微服务空间。以下主要针对平台主体的四层核心模块展开分别介绍。

5.1.1. 应用层

移动终端安全管控平台应用层主要由智能终端 APP 和控制台 Console WEB 构成。

5.1.1.1. 终端 APP

终端 APP 为适配 Android/HMS（鸿蒙 OS）的专用应用，主要由 MDM 管控引擎模块与界面功能模块构成，界面功能模块主要包括首页、个人中心、应用商店、消息中心四部分。

终端 APP 主要实现设备从注册/激活、接收策略、执行管控、常用应用集成、状态实时查询等能力。其中首页中包括扫一扫、设备状态、扫码寄存、申请休假、合规状态、同步消息等功能；通过个人中心可以查询当前应用的版本信息、通讯信息，以及提供设备的基本信息、合规状态、策略内容、管理的软件、休假申请入口、隐私协议以及上传手机 LOG 日志等功能；内置专用应用商店，为设备提供绿色健康的应用下载渠道，并为企业专属提供内部办公应用下载渠道；提供消息中心用于接收管控中心的通知消息和其它系统消息。

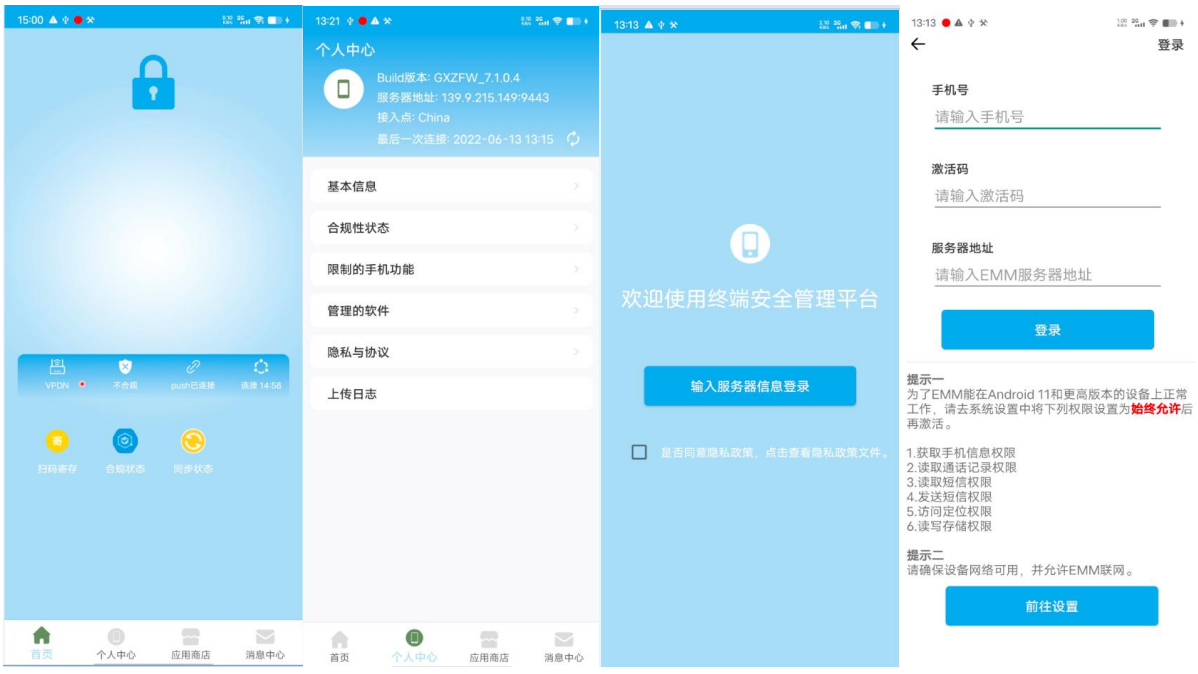


图 5.1.1.1：终端 APP 主要功能界面

5.1.1.2. WEB 控制台

WEB 控制台为管理员和运营/运维人员提供不同权限的操作功能，可以查看设备状态，管理终端用户及组织架构，下发策略 / 应用 / 配置，对设备进行远程控制等，实现对移动设备的全面管理。主要功能模块包括：统计仪表盘、用户管理、设备管理、应用管理、策略管理、审计管理、系统设备七大板块；同时，运维控制台还有部分运维专属能力，包括个性配置、客户端管理和系统参数设计三大模块，具体内容请参考平台用户手册。

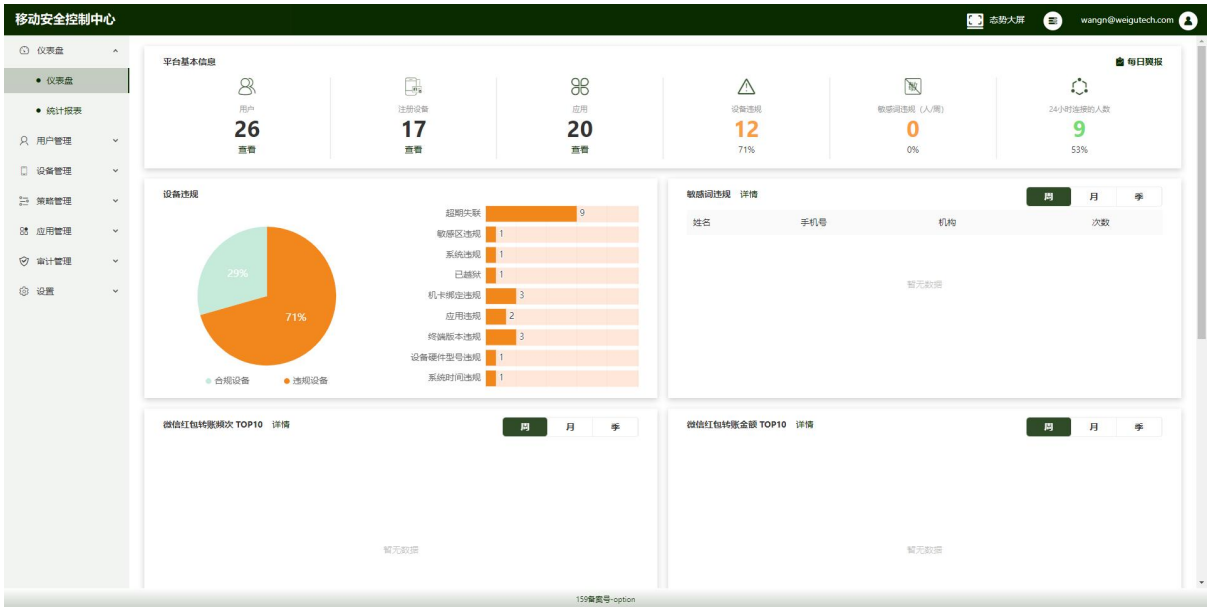


图 5.1.1.2-1：WEB 控制台管理首页

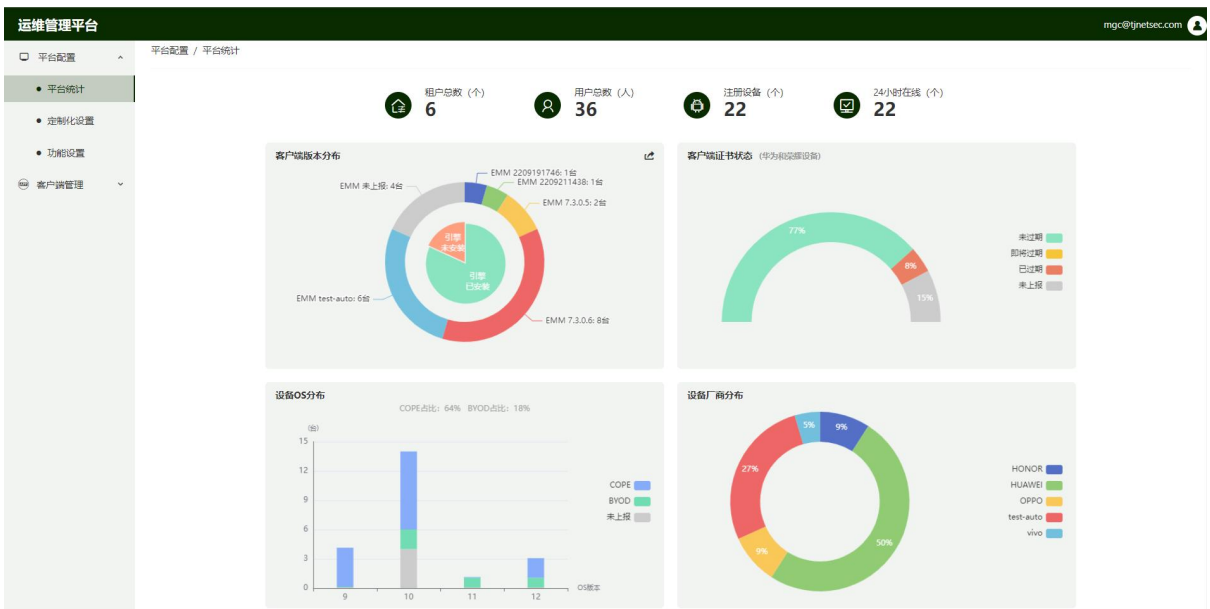


图 5.1.1.2-2：运维管控台

5.1.2. 网关层

安全网关为企业用户远程安全访问内网应用提供服务，利用 Nginx 反向代理、HTTPS、RESTful、SSL、VPN/VPDN 等技术组件，通过构建双向应用授权证书校验和用户身份识别，实现终端安全接入、应用安全接入、用户安全接入的能力。

安全网关工作在“传输层”，可通过用户身份认证，以及“非对称与对称”相结合的加密技术，建立由客户端应用程序到企业内网应用服务器端的“按需”安全连接。使用户可通过任何设备和网络从远程安全地接入应用服务器。特有的“反向代理”功能，使应用服务器安全地保存在企业数据中心内，有效的避免暴露企业内网应用服务器地址，从而保护敏感信息并增强企业安全性。

5.1.3. 业务层

业务层主要由用户管理、设备管理、应用管理、安全审计、身份认证、配置管理、策略管理、远程控制、消息推送、管理控制台等模块组成。

5.1.3.1. 用户管理模块

用户管理模块实现终端用户与管理员用户两套认证授权体系，实现终端用户的管控登记注册与客户端的激活认证；实现管理控制台的授权访问和权限设定。同时，建立终端用户的多级组织架构，并对不同级别的组织节点分别进行策略绑定和权限控制。

5.1.3.2. 设备管理模块

设备管理模块主要负责对终端设备进行信息登记和数据采集，针对终端设备构建资产清单，并实现终端与管控策略的绑定。

5.1.3.3. 应用管理模块

应用管理模块负责构建终端应用白名单和为终端提供可下载安装的绿色 APP 列表清单，为客户端应用商店提供数据支撑和应用分级权限控制。

5.1.3.4. 安全审计模块

安全审计模块为管控终端和系统平台提供分类日志记录能力，采集到的日志数据经过安全审计模块进行归类统计，并以清单的方式展现。主要审计日志有：平台操作日志、敏感词日志、通话日志、短信日志、微信内容日志、支付宝审计日志、翻墙联网日志、防沉迷日志、照片位置屏蔽日志等。

5.1.3.5. 身份认证模块

身份认证模块主要负责对终端设备和终端用户进行身份认证，确保终端设备、管控 APP 和当前用户的身份确定和唯一，通过密码口令和系统安全令牌实现认证机制的安全可靠。

5.1.3.6. 配置管理模块

配置管理模块负责对系统平台用到的配置文件以及客户端个性化参数进行记录和提供服务，为客户端和管理平台提供参数化管理工具。

5.1.3.7. 策略管理模块

策略管理模块负责对终端设备提供配置化工具和同步机制，实现终端策略的有效推送、状态跟踪、执行反馈、策略更新等功能，并针对策略与设备、策略与用户、策略与组织、策略与移动操作系统平台建立一对多绑定关系，为管理员提供多态配置方案服务。

5.1.3.8. 远程控制模块

远程控制模块主要实现管理控制台主动发送指令到某个终端设备的能力，通过 PUSH 消息技术把终端管控策略或其它指令动作，比如获取设备位置等指令，有效推送到终端设备，再由终端 APP MDM 管控引擎解析并执行。

5.1.3.9. 消息推送模块

消息推送模块为解决 Android 终端设备各个 OS 厂商不统一问题，建立的一个统一的推送模块，利用常见 OS 厂商推送渠道与私有 TCP 协议技术，构建了统一的消息

推送路由和引擎，最终实现各个 Android 终端设备有效接收服务端消息通知的能力。

5.1.3.10. 管理控制台模块

管理控制台模块主要为管理员提供 WEB 访问服务，通过 WEB2.0 技术，应用 VUE 前端框架为管理员提供跨浏览器的 WEB 服务，并通过管理控制台实现对整个平台的管控操作。

5.1.4. 技术支撑层

技术支撑层主要由两部分组成，公共技术组件和平台支撑组件，实现对整体平台业务的技术支撑能力，每个模块的主要作用如下。

5.1.4.1. 公共技术组件

1. Tomcat Java WEB 程序运行容器；
2. MQ 消息队列；
3. Spring Java 运行开发框架；
4. 二维码 二维码解析组件；
5. 短信 短信网关组件；
6. PostgreSQL 开源关系型数据库；
7. MongoDB 分布式文件数据库；
8. 加密算法 包括国产加密算法 SM2、SM3、SM4 和国际加密算法 AES、RSA、MD5；

5.1.4.2. 平台支撑组件

1. MDM 移动策略指令控制组件，为终端和管理控制台提供终端远程控制、策略下发、终端数据采集等服务；
2. MAM 移动应用管理控制组件，为终端和管理控制台提供应用列表维护、应用下载、应用推送、应用市场等服务；

3. MIA 移动信息审计控制组件，为管理控制台提供日志记录、分类、查询等服务；为终端提供日志筛选、记录、汇总等服务；
4. Pitcher 适配路由控制组件，为推送指令路由正确的推送渠道；
5. Console 管理控制台组件，为 WEB 管理控制台提供服务支撑；
6. PUSH 消息推送服务组件，为无推送渠道或无法连接互联网服务的终端设备提供 Android 通知推送服务；

5.2. 技术架构

移动终端安全管控平台采用统一集成和插件化服务扩展的技术架构，主体开发语言为 Java，使用数据库集群提供关系数据存储能力，使用消息队列提供异步数据传输能力，使用分布式文件数据库实现信息写入和查询高并发能力，基于 MVC 架构构建主体程序控制系统，并使用自主研发的基于 TCP 的消息引擎实现 Android 平台的主动推送服务。具体架构图如下：

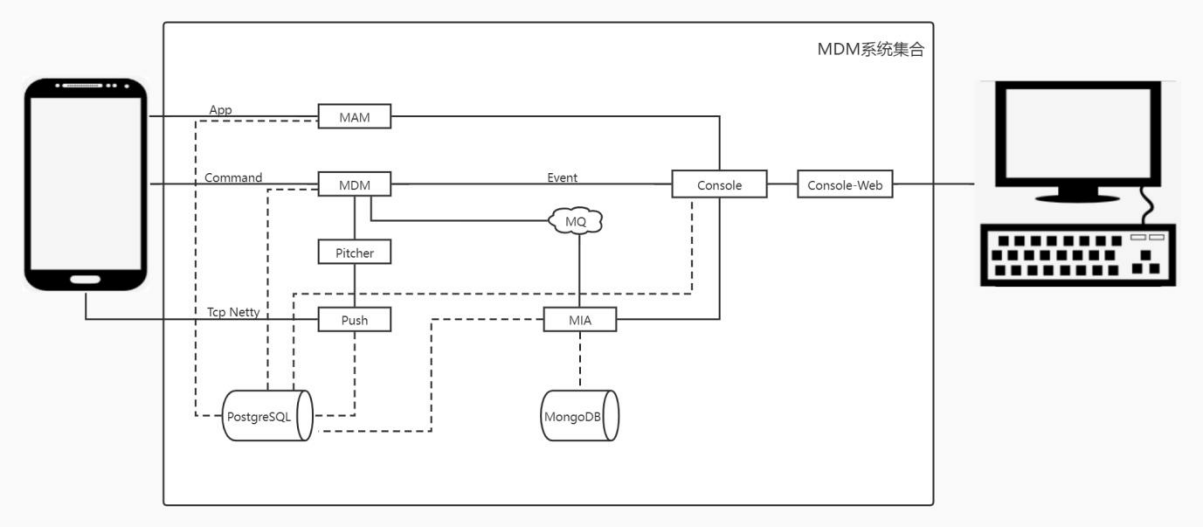


图 5.2：技术架构

移动终端安全管控平台主要由移动应用管控（MAM）、移动终端管控（MDM）、路由适配（Pitcher）、消息推送（Push）、数据库（PostgreSQL）、消息队列（MQ）、日志审计（MIA）、分布式文件数据库（MongoDB）、控制台逻辑服务（Console）和控制台 WEB 服务组成。

客户端通过三类通讯交互实现终端管控、应用安装和推送消息接收的功能，控制台由管理员通过浏览器访问 WEB 站点的形式使用。控制台采用 B/S 架构有利于轻量化、跨平台和异构集成；终端应用采用 C/S 架构构建，有利于实现终端管控权限调用。

5.3. 总体业务流程

移动终端安全管控平台的总体业务流程如下：

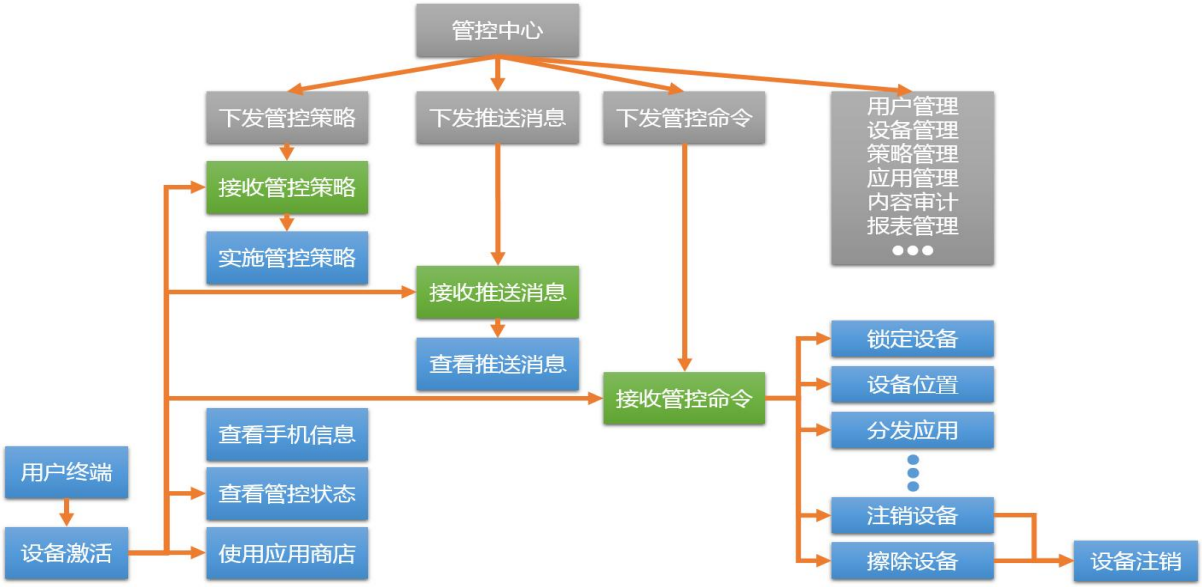


图 5.3：业务实现流程

移动终端安全管控的核心是针对政企用户终端强管控和终端审计的需求，通过深入理解政企客户的日常管理特点，平台有针对性的进行了功能的开发和优化，提供了一整套功能完善、业务闭环、适配快速的解决方案。

5.4. 软件流程

5.4.1. 策略管理流程

管理员通过 WEB Console 新增或修改策略后，通过 MDM 模块路由消息通知，再由消息推送模块发送通知到相应终端上，终端 APP 接收到通知后解析并识别策略下载地址，终端 APP 发起主动请求下载当前策略信息，增加或覆盖策略，最后上传策略执行情况。

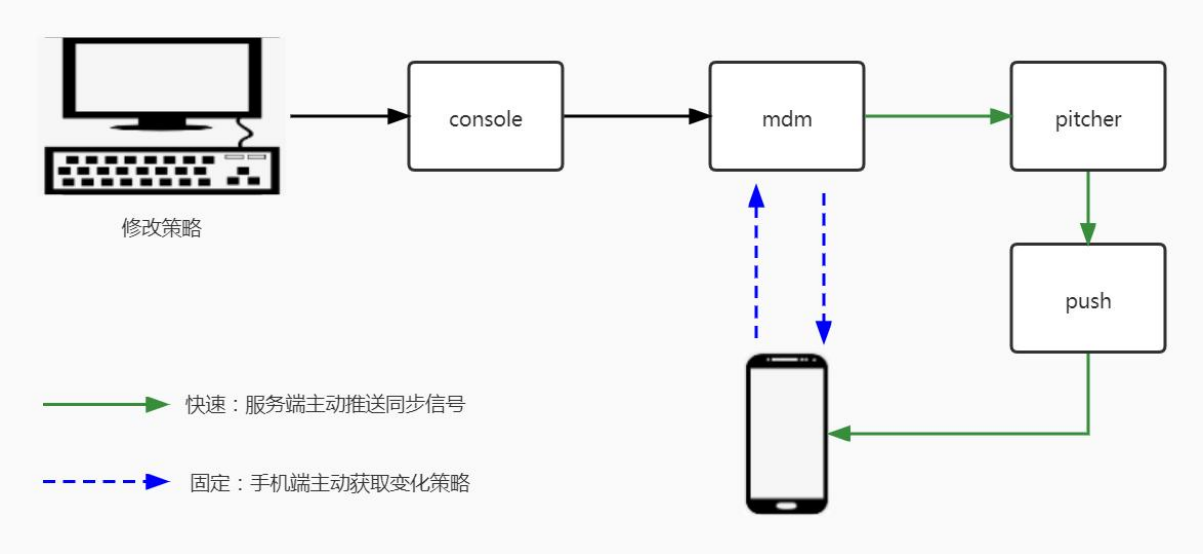


图 5.4.1：终端管控策略下发同步流程

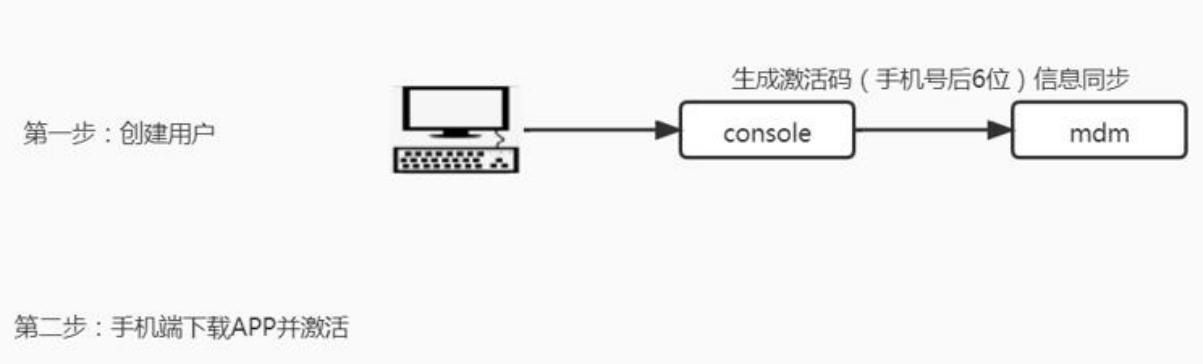
5.4.2. 设备激活流程

第一步先由管理员创建新用户用于生成激活码来绑定设备；

第二步前置条件是用户先下载安装好终端 APP 应用，当终端 APP 安装成功后会自动启动 PUSH 接收模块，与 PUSH Server 建立长连接；然后用户根据管理员新增的用户进行注册登录，设备与当前策略列表进行绑定；终端 APP 再检查与自身有关的应用策略，并加载执行；

第三步 MDM 模块定时监测策略的活动状态，并进行实时推通知到终端 APP；

第四步终端 APP 收到策略推送通知后及时拉取策略信息；



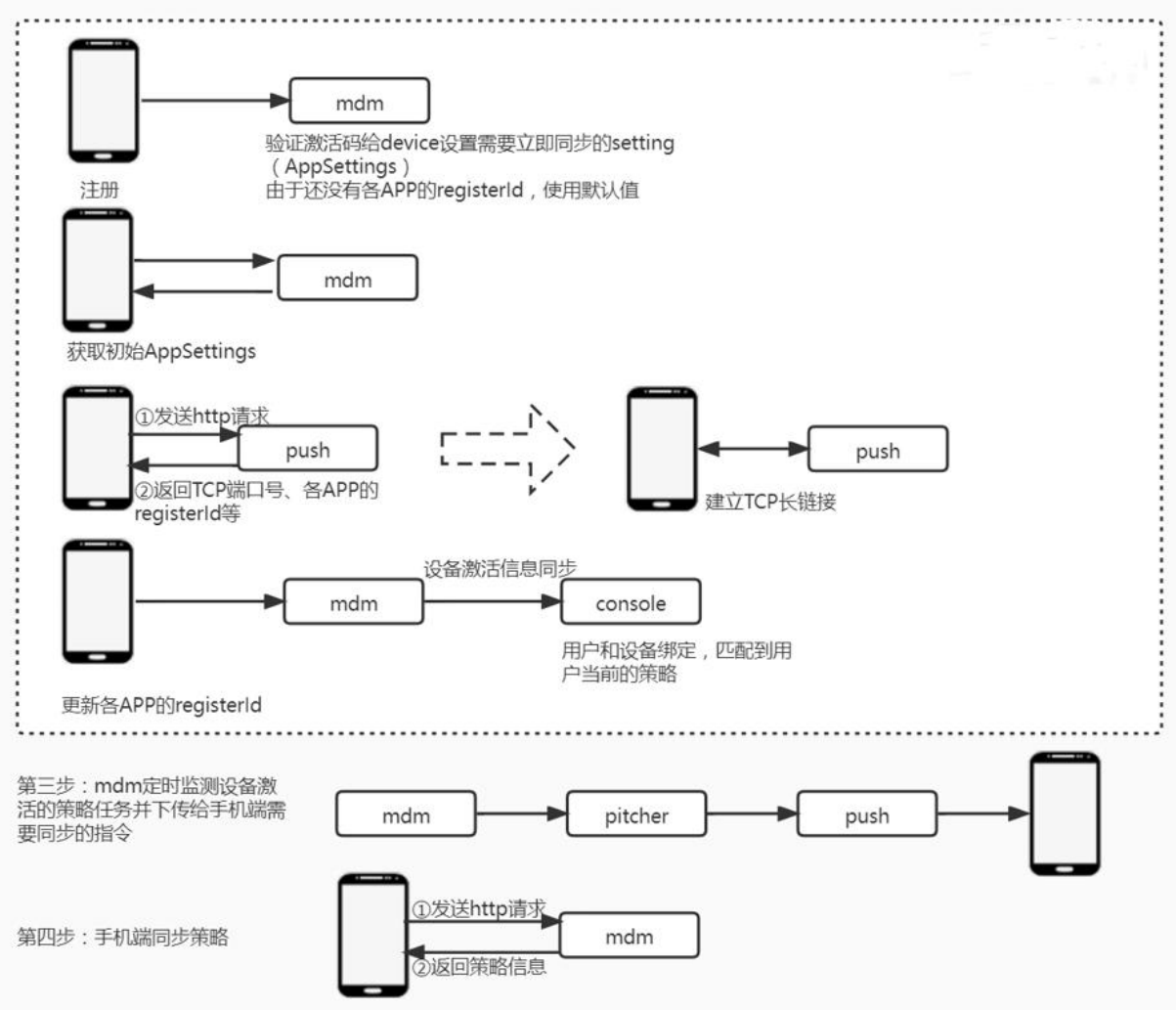


图 5.4.2：设备激活流程

5.4.3. 设备注销流程

设备注销的流程分为两种场景，分别是场景一由管控后台发起注销流程；场景二由客户端发起注销流程。

场景一：管控后台发起 MDM 指令到终端 APP；终端 APP 收到注销指令后执行注销动作并返回服务端注销指令执行结果；

场景二：客户端自助注销后通知 MDM 服务端；服务端及时更新当前设备状态；

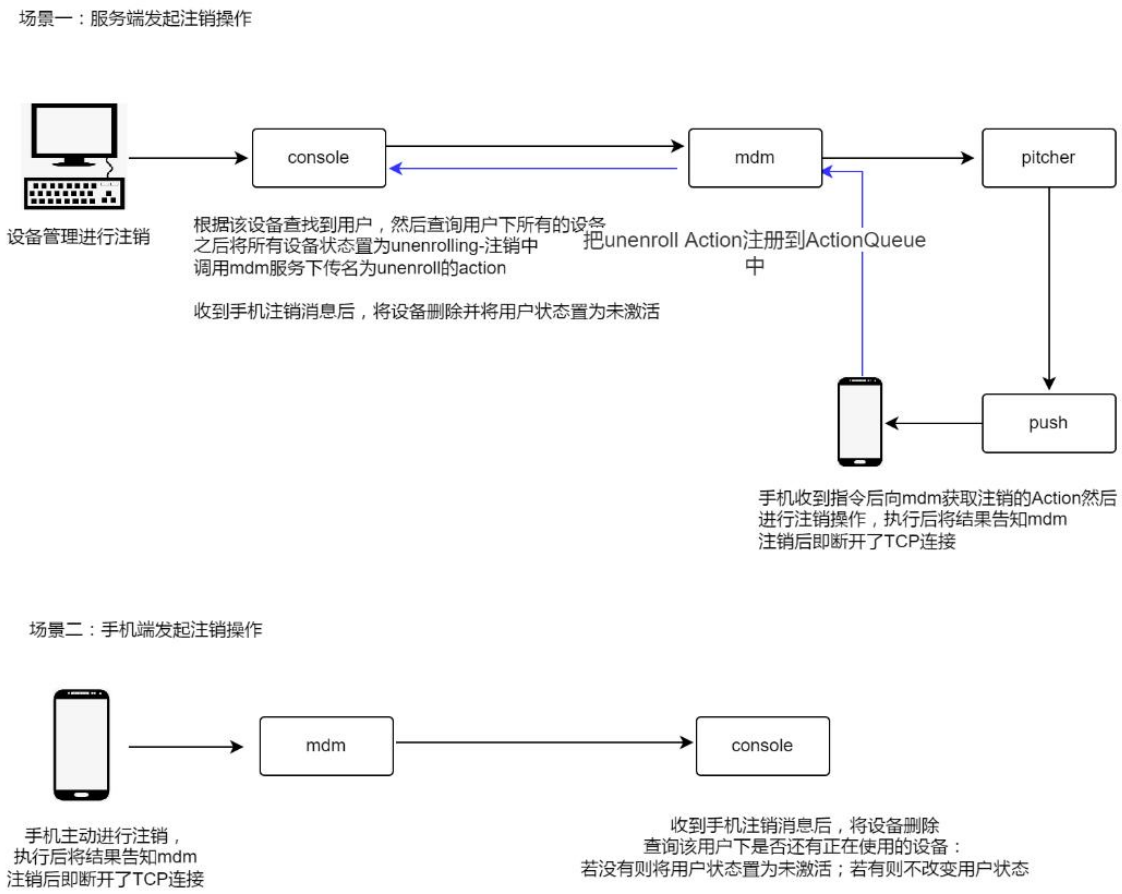


图 5.4.3：设备注销流程

5.4.4. 应用管理整体流程

应用上传：应用上传分为本地上传和云端上传，本地上传直接由管理员通过 Console WEB 进行上传，应用保存到 MAM 模块中；云端上传是由管理员通过选择好 APP 市场中的应用后，由 MAM 自动下载云端应用到服务器；

应用删除：由管理员通过 Console WEB 直接删除 MAM 模块中的应用；

静默安装/卸载：由管理员配置好静默安装或卸载指令策略后，MDM 通过路由推送策略指令到终端 APP，终端 APP 收到指令后获取当前策略并解析，最终通过自动连接 MAM 下载安装 APP；

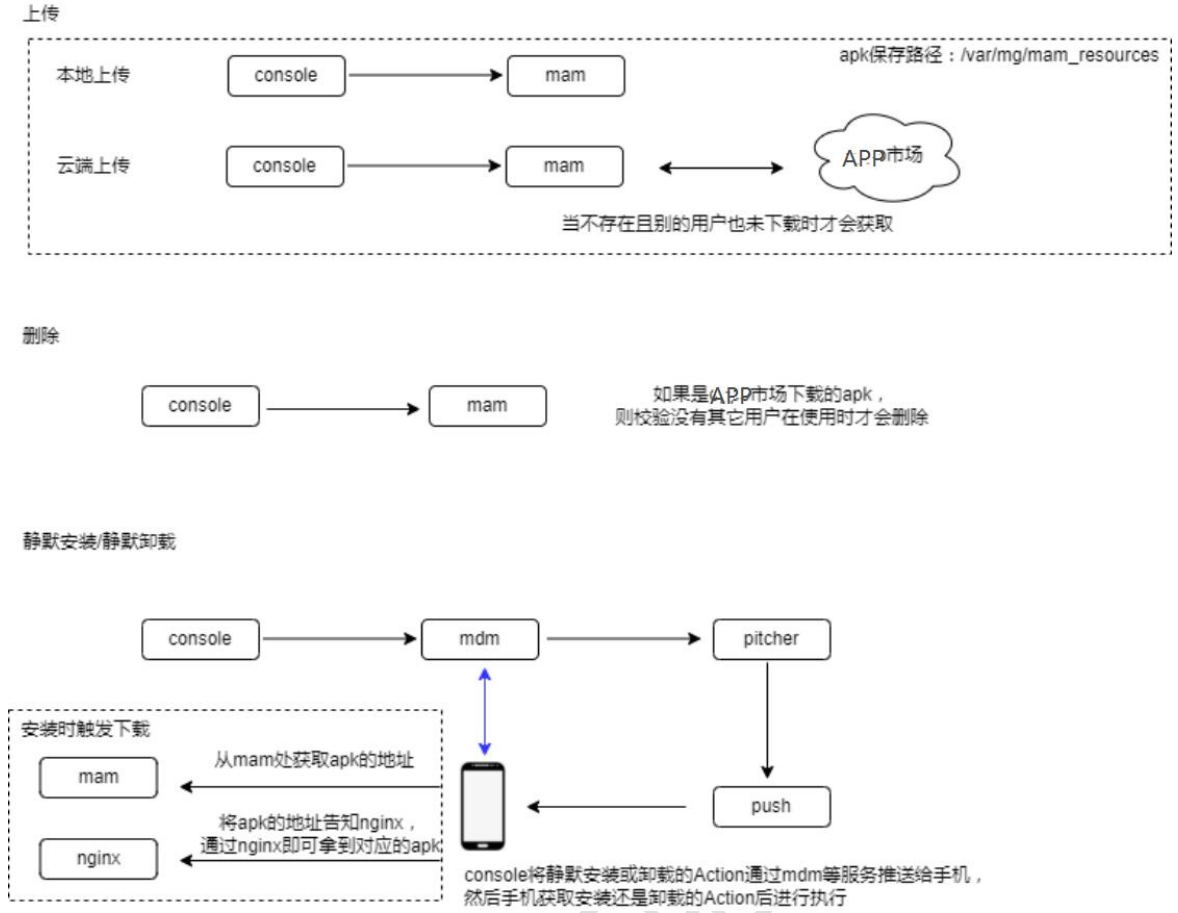


图 5.4.4：应用生命周期管理流程

5.4.5. 审计日志数据流程

第一条流程是由终端 APP 加密数据并上报到（1）MDM 模块，MDM 存储数据到（2）MQ 队列，再由（3）MIA 模块从 MQ 读取消息，最后消息存储到（4）MongoDB；

第二条流程是由管理员通完（8）Web Console 查询审计日志，由（7）Console Server 调用（6）MIA 模块从（5）MongoDB 中读取相关日志信息；

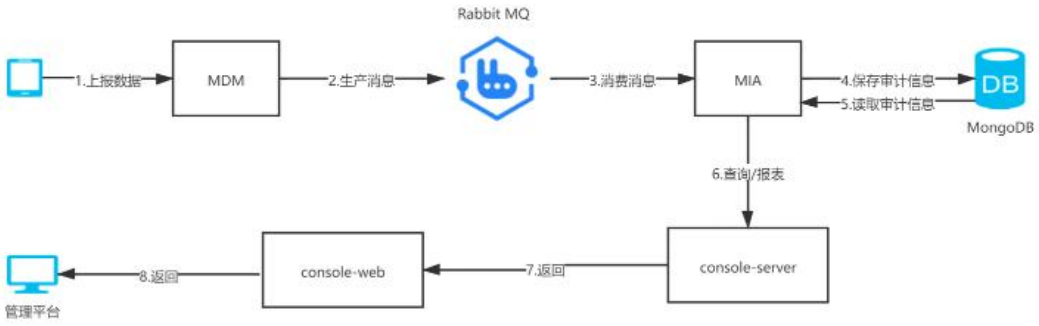


图 5.4.5：审计日志同步流程

5.5. 关键技术解决方案

移动终端安全管控平台利用传统 B/S 与 C/S 相结合的技术架构，利用移动化特色的通知推送、OS MDM 配置化等特性，融合新老技术特性构建了新一代移动终端安全管控平台。有特色的关键核心技术点有 MDM 技术、MAM 技术、MIA 技术和 PUSH 技术。

5.5.1. 移动设备管理 MDM 技术

移动设备管理(Mobile Device Management, MDM)：基于平台的移动设备全生命周期管理，具体包括：终端状态管理、设备外设管控、设备使用管理、设备状态监控、设备合规性检查和终端内容审计等；

该能力通过基于 Android OS 独立的 MDM API 实现，通过客户端 APP 获取 OS 的 MDM 管理权限来调用 MDM API 实现设备的密码、外设、设备状态、行为合规等方面的系统控制；同时，利用 C/S 通讯架构和移动 PUSH 技术，实现后端远程控制设备及设备状态信息实时同步的能力，让移动终端安全管控平台能通过统一管理后台管控多个设备终端。

5.5.2. 移动应用管理 MAM 技术

移动应用管理(Mobile Application Management, MAM)：通过应用商店对各个 App 提供分发、管理和策略控制，同时平台提供 App 使用情况功能；

该能力通过基于 MDM 技术，利用 OTA 空中下载技术实现 OS 上的 APP 安装和更新。同时，基于 MDM 技术，利用 MDM 专属 API 实现应用的静默安装和更新升级。移动终端安全管控平台利用 PUSH 技术下发应用安装、更新、删除指令，终端 APP 通过 OS MDM API 实现 APP 应用的生命周期管理，并下载当前用户的应用黑白名单进行实时监控。

5.5.3. 移动 MIA 技术

移动设备信息审计(mobile device information auditing，MIA)：信息审计采用数据加密技术，严格控制设备端采集数据到服务端日志审计端到端加密，平台细分管理角色为管理员、子管理员、操作员和审计员，各角色分权分域对用户设备和信息审计分别进行管理；

该技术利用 MDM 权限有效采集移动端设备完整信息数据，包括设备信息、应用信息、用户操作行为信息、个别应用通讯信息、个别应用支付信息等，利用端到端安全加密技术，实现数据采集、传输、存储、使用全过程的安全防护，为用户提供多维报表服务和安全态势分析的数据支撑来源服务。

5.5.4. 平台消息推送 PUSH 技术

平台消息推送（PUSH)：独立的消息推送引擎，负责进行信息推送、公告或资讯推送等功能。

该技术利用自主设计的私有通信协议技术，实现 Server 后端主要发送通知消息到 Client 客户端的能力。客户端通过一个长时的心跳长连接保持一个 TCP 网络通道，服务端可以主动推送一个内容较小的 Payload 消息体，由客户端解析后再启动进程按消息体默认的协议进行二次请求来获取服务端更多的信息内容。因此通过该技术，理论上可以实现任意大小文本、文件的主动推送。

5.6. 重要功能实现方法

移动设备管理，又称 MDM（Mobile Device Management)，它提供从设备注册、激活、使用、淘汰各个环节进行完整的移动设备全生命周期管理。

本平台利用基础的 Android device policy controller（DPC）API 库进行基本的设备管控操作，并针对国内设备厂商提供的不同机型和 OS 版本进行适配，获得平台厂商授权管控 MDM 证书后，通过配置终端 APP 为 DeviceOwner 权限来获得设备所有

者身份，最后利用 Android SDK 调用相应管控 API 实现终端的安全管控，示例代码如下：

禁止/允许截屏

```
private void setScreenCaptureDisabled(ComponentName admin, boolean disabled) {
        if(isProfileOwnerApp) {
            mDevicePolicyManager.setScreenCaptureDisabled(admin, disabled);
        }
    }
```

是否禁止截图

```
private boolean getScreenCaptureDisabled(ComponentName admin) {
        boolean res = false;
        if (isProfileOwnerApp) {
            res = mDevicePolicyManager.getScreenCaptureDisabled(admin);
        }
        return res;
    }
```

6.产品功能

6.1. 移动设备管理

平台提供了基于移动设备全生命周期的管理方案，从设备的获取、部署、运行以及回收四个生命周期环节提供了完善的管控策略和工具。主要功能模块有：用户及组织管理、身份认证、终端安全加固、设备远程控制、设备限制策略、审计管理、通信限制、应用黑白名单、敏感词过滤、日志上报策略、合规策略、时间围栏、地理围栏等功能模块。

MDM 同时兼顾企业统一配发设备 COPE（Corporate-Owned，Personally Enabled）和自带设备 BYOD（Bring Your-Own Device）的特点。在确保安全性的同时，不影响移动终端的用户使用体验。

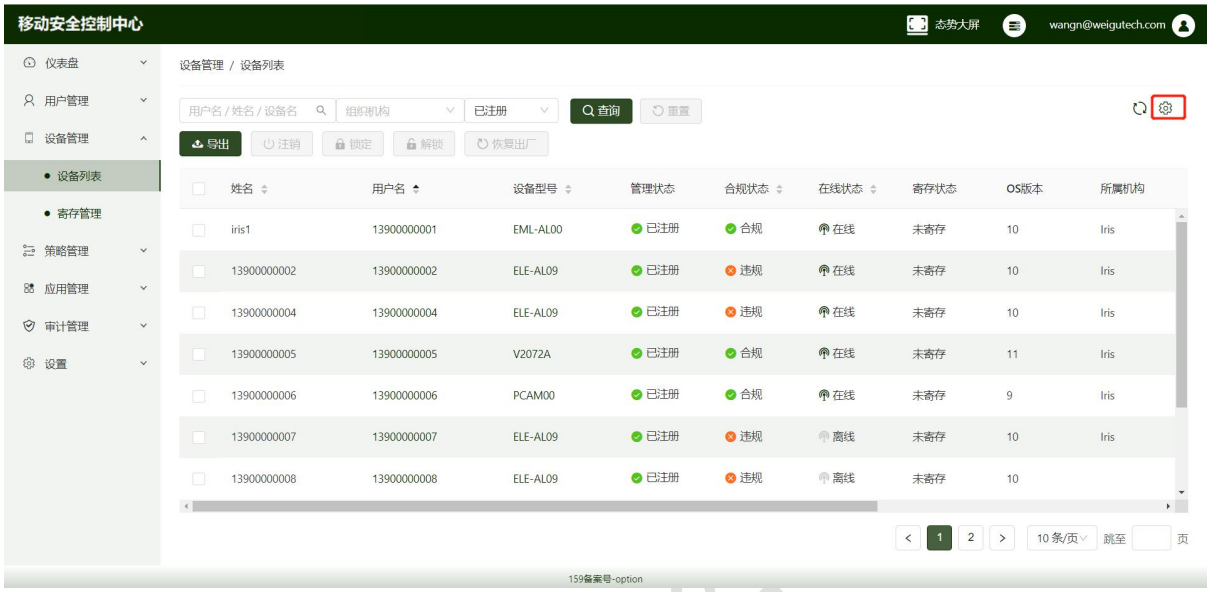


图 6.1：移动设备管理

6.1.1. 用户及组织管理

移动终端安全管控产品提供批量用户及设备导入功能，支持 API 同步导入方式。通过管理平台能方便地对所有用户及设备进行查询，实时了解用户及设备的详细情况，以便企业对移动设备的监测和管理。如员工离职，管理员可将用户从管理平台中禁用并删除。

平台以用户为基础，逐步建立分级独立的管理层级，即组织部门、角色组/用户组、用户的三层管理结构。所有的设备、应用以及安全策略管理，都可以针对用户、角色组合及组织机构进行多维度管理，大大简化了用户管理难度，方式灵活且针对性强。

系统支持横向多租户管理，租户间数据完全隔离；又同时支持租户内按照组织机构纵向隔离，设置机构管理员分管各自机构，做到组织机构分级分权管理。

在平台的用户管理模块中，有丰富的用户管理策略和方法，比如按组织架构节点发送消息，在用户模块选择用户/用户组后直接发送消息，用户下的所有已激活设备将会

收到消息，管理员发送的消息记录还会保存在操作日志里随时查看；

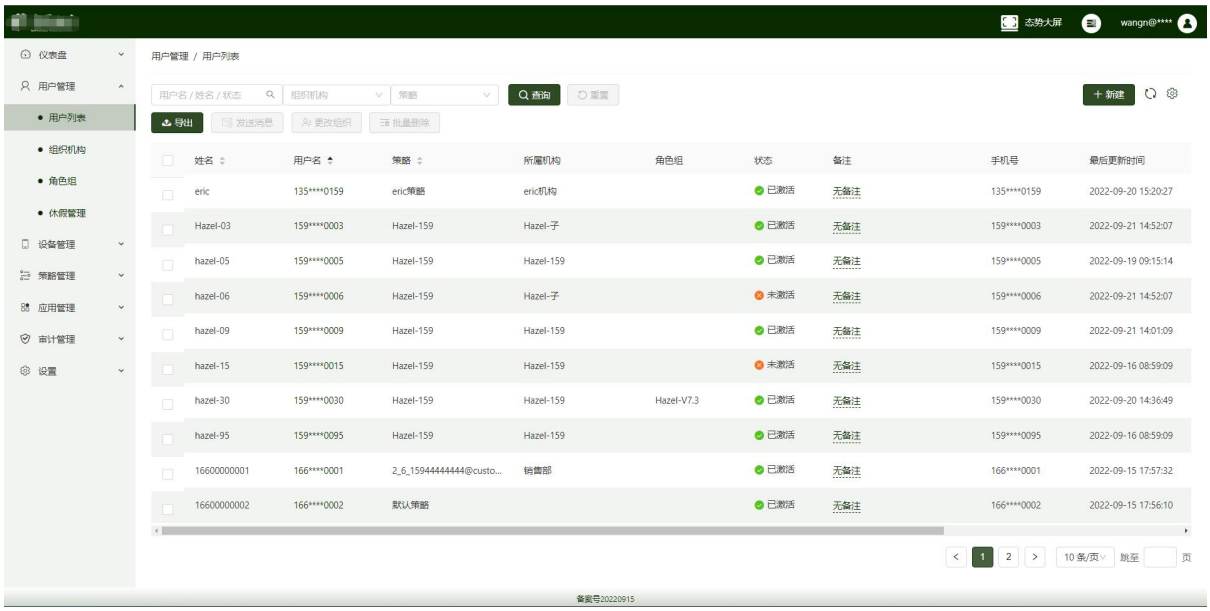


图 6.1.1-1：用户管理

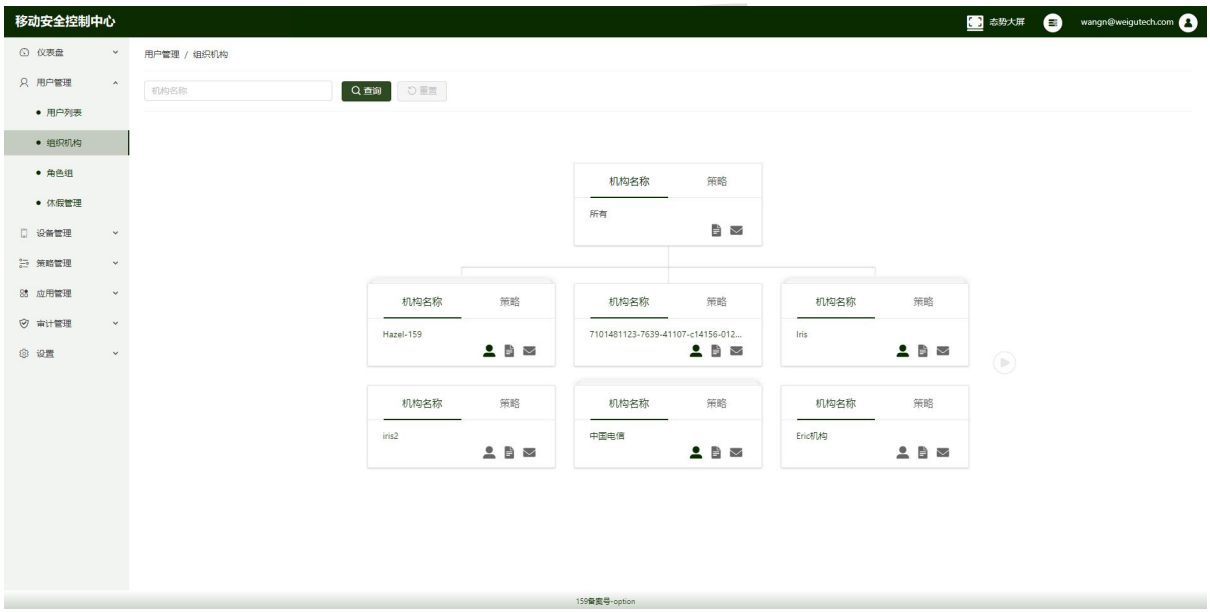


图 6.1.1-2：组织架构管理

6.1.2. 安全上网通道

在移动数据通道方面，可以由运营商为政企组织提供了无线 VPDN 业务服务。无线 VPDN 业务利用 L2TP 隧道技术为客户构建的与公众互联网相隔离的虚拟专用网络。

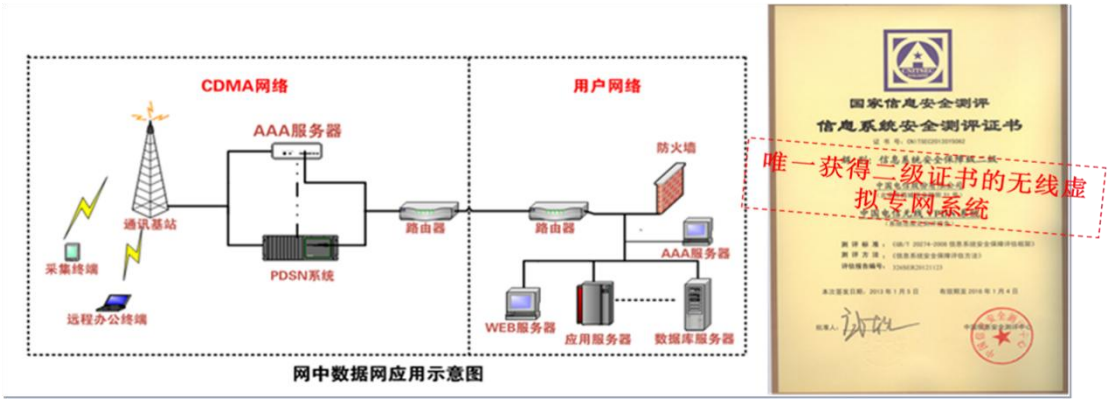


图 6.1.2：VPDN 业务网络结构图

基于专有的 VPDN 网络，组织成员在智能手机上安装移动应用，管理员对智能手机下达的管控指令等数据传递都是在与外界隔离的网络环境下完成，防止了数据被监听、被篡改、被破坏。

一方面在初次检测到手机卡被插入时，智能手机会自动添加有关 VPDN 参数的 APN 配置（前提条件是手机可以识别出手机号），避免了人工对每部手机进行配置的工作；另一方面，为了保证网络接入的安全，需要定期变更连接 VPDN 网络所需要的密码时，可以通过手机管理平台进行 APN 的密码修改，平台主动将 VPDN 参数的变化量推送到每部手机中。

6.1.3. 终端安全加固

本方案对智能手机进行深度定制，从底层杜绝 ROOT 和刷机的行为，在手机启动时对每层 bootloader 启动的应用进行完整性校验，避免在系统层面混入恶意的移动应用。为了避免手机预装应用中存在着可能引起泄密的移动应用，对预装应用也进行了定制筛减。此外，一旦发现手机被 ROOT，系统自动进行违规处置，上报信息和锁定设备。

成员使用的智能手机必须在组织的严格管控之下，绝对不允许出现手机脱离管控的情况发生。为此，本平台对以下可能脱离管控的情况制定了相应的策略，如

- ✓ 防刷机：已经提供了防刷机的功能，确保不会被替换为非法版本。
- ✓ 防恢复出厂设置：屏蔽恢复菜单，确保不会被初始化。

- ✓ 防换卡：非组织用卡放到手机上无法上网，并通知管理平台。
- ✓ 客户端的卸载：在组织定制手机中预装的安全应用商店、手机管理客户端以及浏览器均定制为系统级的应用，在手机进行防 ROOT 处理后，这些应用已经不能被卸载，确保终端受控。

6.1.4. 设备远程控制（信息防泄露）

当手机丢失时，手机中保存的数据很可能会泄漏。为了避免这种风险，管理者可以远程变更解锁密码并锁定智能手机，也可以远程擦除或恢复出厂设置智能手机上的数据。而如果手机被找回，还可以远程对手机进行解锁操作。

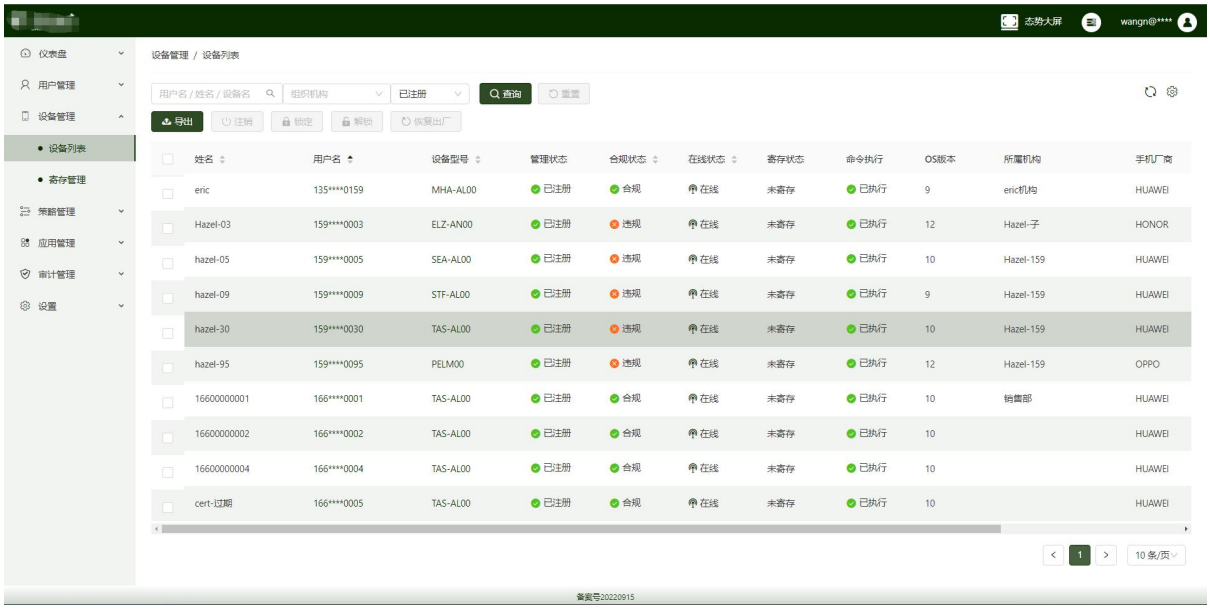


图 6.1.4：设备远程控制

6.1.5. 设备远程策略管控

移动终端安全管控平台利用远程控制技术，下发设备管理策略集到相关用户或用户组设备中，针对不同用户管控要求可以分别配置对应策略，终端 APP 接收到策略后根据策略的配置管控当前设备，并在出现违规行为时根据策略配置采取相应处置方式。

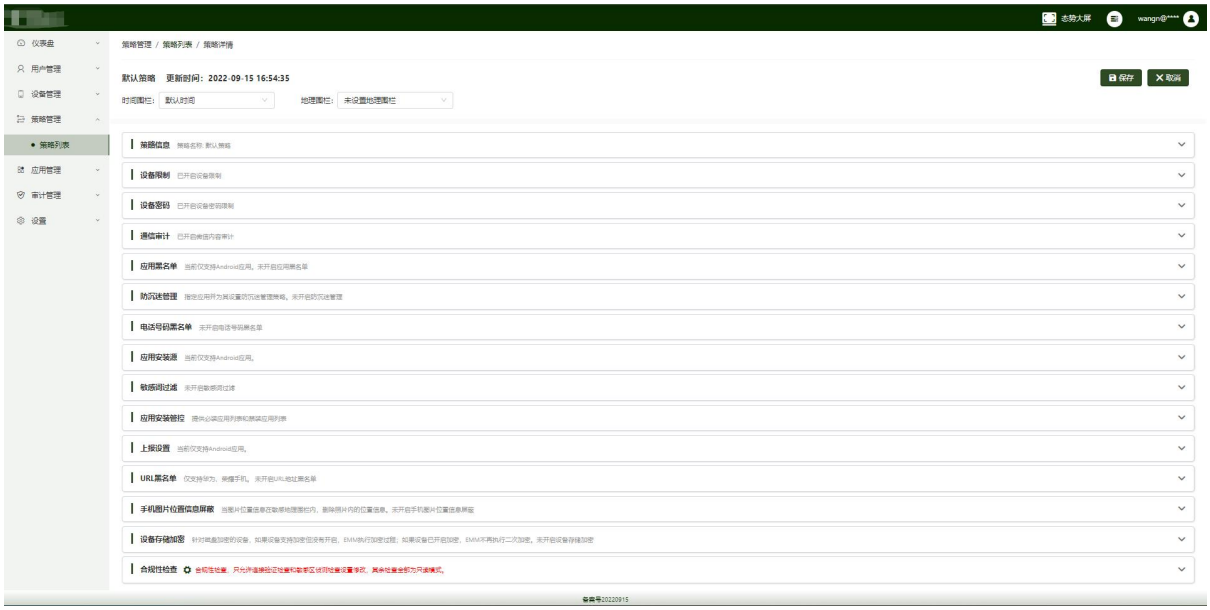


图 6.1.5：策略清单

策略整体包括十五个分类，分别为策略基本信息、设备限制策略、设备密码策略、通信审计策略、应用黑白名单策略、防沉迷管理策略、电话号码黑名单策略、应用安装源策略、敏感词过滤策略、应用安装管控策略、上报设置策略、URL 黑名单策略、手机图片位置屏蔽策略、设备存储加密策略和合规性检查策略。

6.1.5.1. 设备限制策略（外设强管控）

本平台可以为政企组织提供适配智能终端，该终端将摄像头、WiFI、蓝牙、USB、GPS 等容易泄密的外设进行初始化禁用，同时具备相关外设的管理接口可实现 31 项具体管控细项。

手机管理平台利用这些 API 接口实现了在平台上对这些外设进行开启和关闭的管理，一方面避免了通过这些外设造成信息机密泄漏的风险；另一方面也可以在特殊情况下，经过组织领导的审批，向成员开启这些外设。

图 6.1.5.1： 设备限制策略

定制手机可以对 SD 卡和第二手机卡槽进行了底层禁用，禁止在手机中插入 SD 卡，禁止在第二个卡槽中插入手机卡。

6.1.5.2. 通信限制及审计管理

为政企组织提供在禁用或强制开启的主副卡通讯策略，并对通话记录和短信等进行日志审计，见下图。

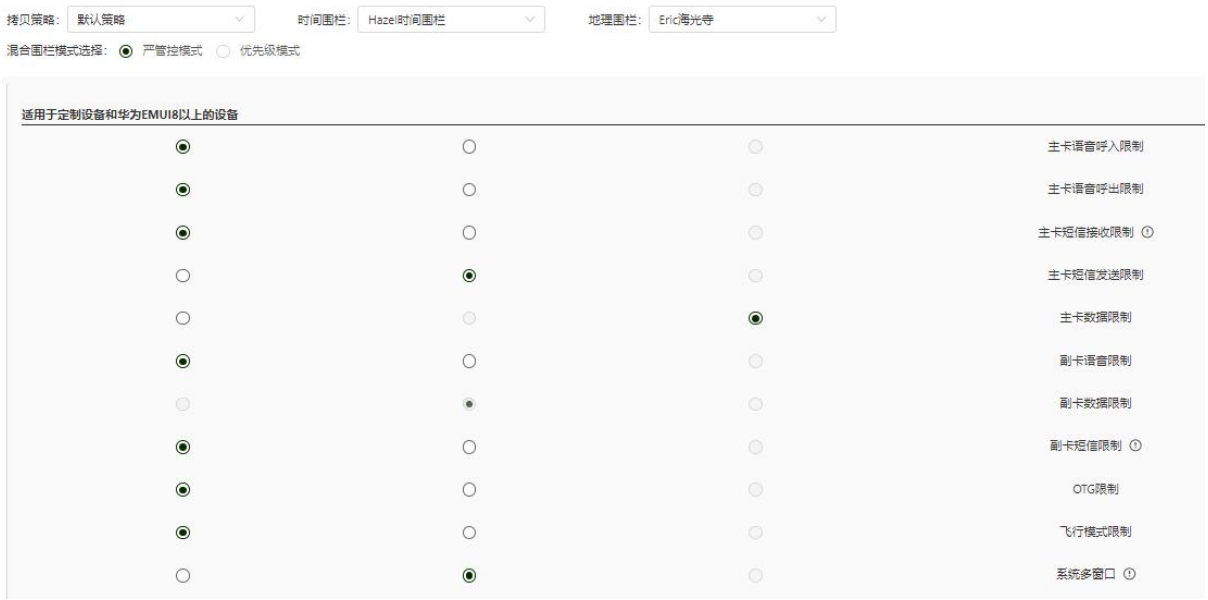


图 6.1.5.2-1：呼入呼出限制策略

图 6.1.5.2-2：手机管理平台对呼入呼出的限制

6.1.5.3. 设备密码策略

为政企组织强制设定设备终端密码管理策略，并配置强制更新周期保护终端设备的使用安全。

图 6.1.5.3：设备密码策略

6.1.5.4. 应用黑白名单策略

考虑应用黑白名单具备互斥性，因此当一个终端设备设定为黑名单时针对此设备则只限制安装黑名单的应用，反之则只开放安装白名单的应用。

图 6.1.5.4-1：应用黑名单

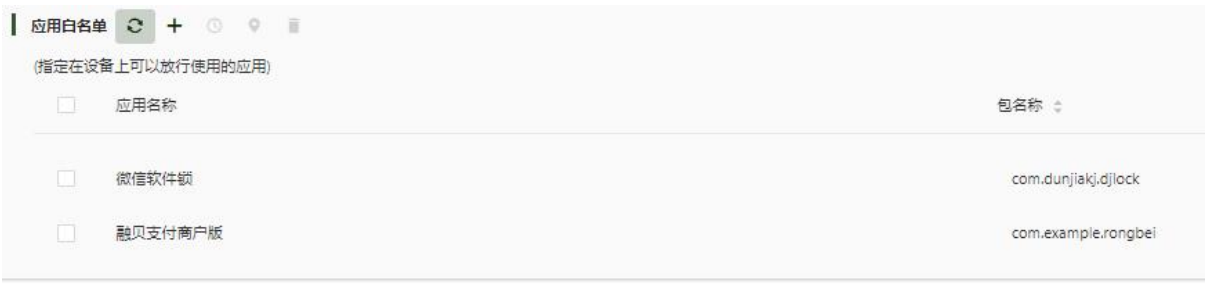


图 6.1.5.4-2：应用白名单

6.1.5.5. 防沉迷管理策略

通过策略设置防沉迷管控，来防止用户沉迷于抖音，游戏等应用，可以设置超时弹窗提醒或禁止使用 app。

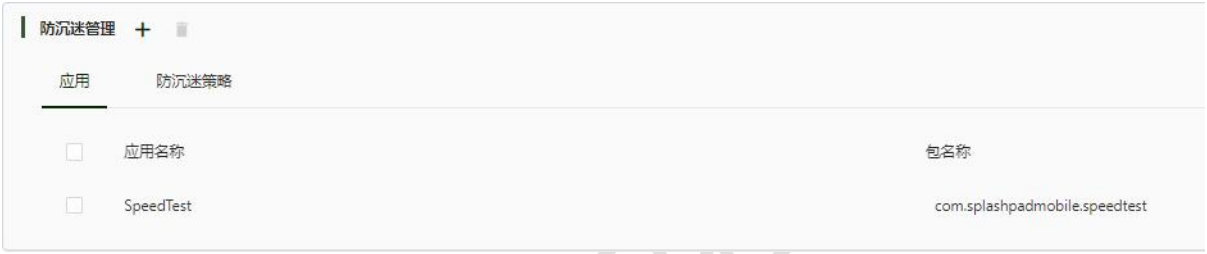


图 6.1.5.5：应用白名单

6.1.5.6. 电话黑白名单策略

考虑电话黑白名单也具备互斥性，因此当一个终端设备设定为黑名单时针对此设备则只限制呼叫/接听黑名单的电话，反之则只开放呼叫/接听白名单的电话。

图 6.1.5.6-1：电话号码黑名单

图 6.1.5.6-2：电话号码白名单

6.1.5.7. 应用安装源策略

控制设备安装应用的授信源地址，默认强制使用移动终端安全管控平台的应用商店下载安装 APP，同时也可以开放官方和第三方经过平台评测过的应用商店。

图 6.1.5.7：应用安装源

6.1.5.8. 敏感词过滤策略

移动终端安全管控平台提供敏感词过滤策略，可以分别针对不同应用提供输入发送过滤和接收信息过滤，现支持微信与 QQ 的接收过滤。

图 6.1.5.8：敏感词过滤

6.1.5.9. 应用安装管控策略

移动终端安全管控平台支持设置终端的必装应用和禁装应用，此策略与应用黑白名单的主要区别是应用是否可以安装，黑白名单中的应用是可以正常安装的，但无法打开使用；而必装/禁装应用控制应用的下载安装。

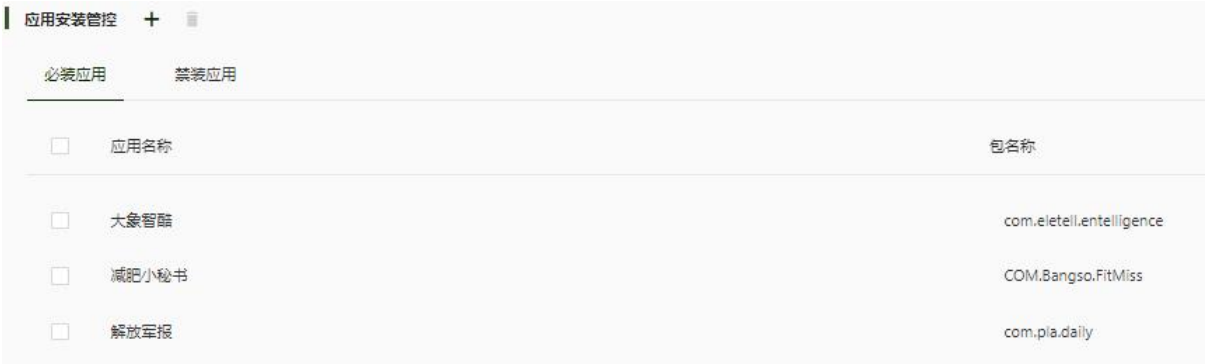


图 6.1.5.9：应用安装管控

6.1.5.10. 日志上报策略

上报策略控制移动终端行为日志的上报周期和频次，通过增量上报的方式及时掌握终端的日常使用行为，为审计模块提供数据支撑。

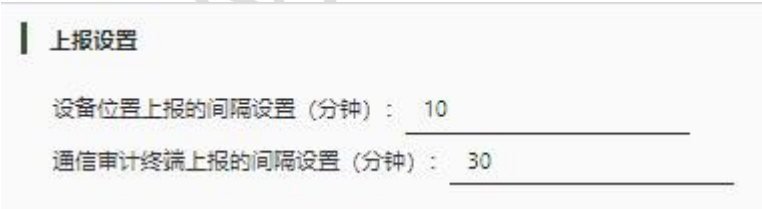


图 6.1.5.10：上报设置

6.1.5.11. URL 黑名单

移动终端安全管控平台可以限制设备的上网行为，通过过滤不合规的 URL 来防止设备访问违法违规网站。

图 6.1.5.11：URL 黑名单

6.1.5.12. 手机图片位置信息屏蔽策略

移动终端安全管控平台通过该功能，可以根据地理围栏进行敏感位置过滤屏蔽，防止敏感信息泄露。

图 6.1.5.12：图片位置屏蔽

6.1.5.13. 设备存储加密

移动终端安全管控平台通过配置强制手机存储加密，可默认强制打开手机终端支持的内部和外部存储器的加密开关，限制条件为智能终端操作系统需要支持持久化存储器加密功能。

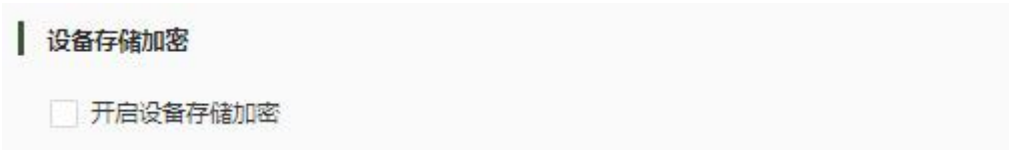


图 6.1.5.13：设备存储加密

6.1.5.14. 合规性检查策略

合规性检查策略为终端设备提供违规后的处置方案，终端 APP 实时根据合规性检查策略来探测设备型号、系统版本、应用限制、越狱探测、网络连接有效性、时间及地

理围栏、机卡违规、终端限制版本等合规参数，一旦发生违规事件，则根据此策略来选择处置方案。

图 6.1.5.14：合规性检查

6.1.6. 时间地理围栏

移动终端安全管控平台提供时间与地理围栏的策略管控方案，可以利用时间围栏、地理围栏和设备策略组合成多元化管控方案，并可以分配多个策略组，用于控制企业人员的一天作息行为。当时间围栏和地理围栏同时选择自定义围栏时，会显示混合围栏模

式选择。混合围栏模式有两种，严管控模式和优先级模式。

严管控模式：时间围栏和地理围栏同时开启时，只要有一个围栏条件满足管控即生效。

优先级模式：时间围栏和地理围栏同时开启时，两个围栏条件均满足管控才生效。

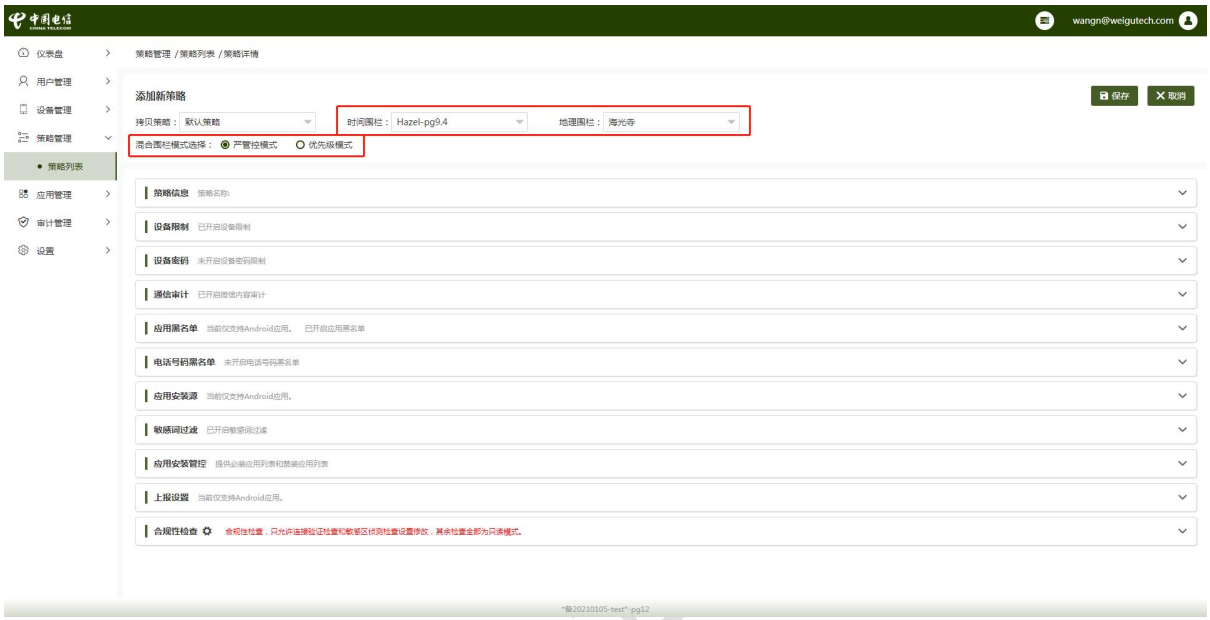


图 6.1.6：时间/地理围栏策略

6.2. 移动应用管理

平台内置预装唯一的安全应用商店，在策略配置下可以仅允许从该应用商店安装移动应用，通过浏览器和其他途径下载的应用将被禁止安装。同时，安全应用商店的移动应用只能通过智能手机综合管理平台进行维护：在管理平台上可以一目了然地了解到每部手机上安装的移动应用的情况；在管理平台上可以对安全商店的应用进行添加、删除等操作；可以指定静默删除某些手机中指定的移动应用；可以为每部手机配置应用黑名单，禁止安装不被允许的移动应用，一旦发现安装了违规应用，则管理平台会自动静默将这些应用卸载掉，同时会记录日志提交违规告警信息。

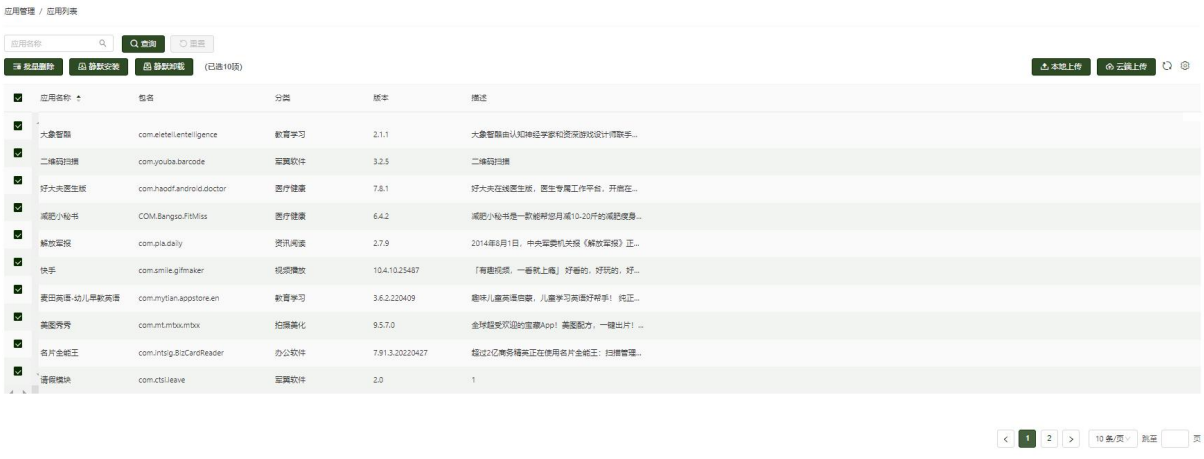


图 6.2： 应用商店管理

6.3. 合规审计

平台提供多种数据可视化的分析报告，主要有设备违规报告，设备风险报告，设备库存使用报告，设备使用情况报告，APP 使用情况报告，用户增长报告等等，实现了报表查看、报表导出、报表订阅的全方位操作。也为管理员提供可视化数据大屏，更直观地展示当前设备运行状态及用户上网行为的趋势分析。

审计分类包括平台操作日志、敏感词日志、通话日志、短信日志、微信内容日志、支付宝审计日志、翻墙审计日志、防沉迷日志、照片位置屏蔽日志八大分类。

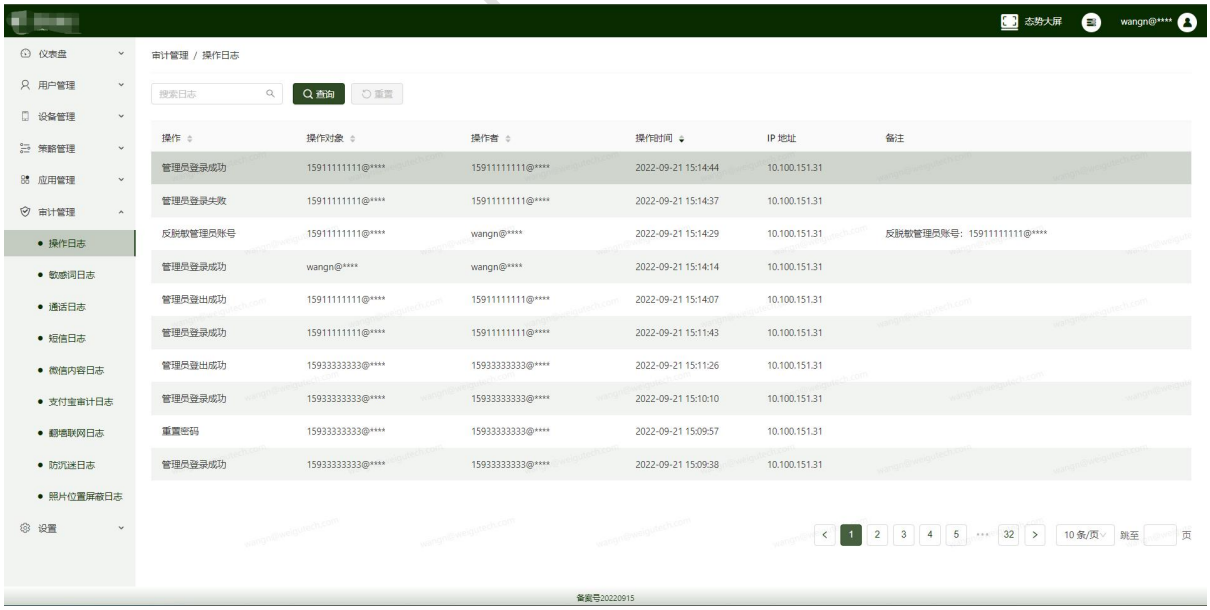


图 6.3：合规审计

6.4. 个性风格的平台配置

为组织提供的终端开关机画面、壁纸等按照组织要求进行了定制，也可以配置平台的登录背景和显示 LOGO，可以在背景图库中也预置了个性题材的图片，体现组织用机的特色。

图 6.4：个性化平台配置

6.5. 平台数据仪表盘

平台提供多种内容丰富的图形化、数据可视化的分析报告，主要有设备违规报告，设备风险报告，设备库存使用报告，设备使用情况报告，EMM 客户端使用情况报告，应用使用情况报告，用户增长报告等等。管理员可以对用户、设备、应用使用情况、设备风险及违规情况进行有效分析，直观地对违规人员进行管理，同时可以导出各类信息报表作为各类报告的素材。实现了报表查看、报表导出、报表订阅的全方位操作。

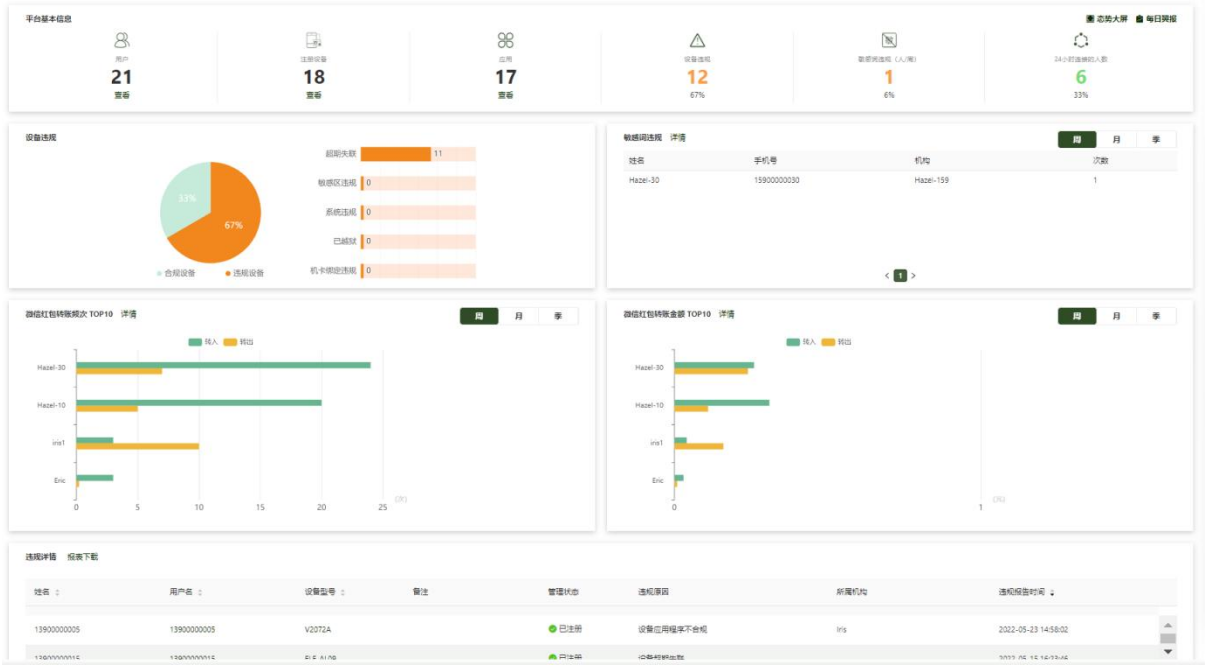


图 6.5-1：平台仪表盘

所提供的报表包括：违规告警记录、内容审计记录、用户统计记录、设备统计记录、应用安装统计记录等。

图 6.5-2：数据统计导出

6.6. 运维管理控制台

平台为运维人员提供运维管理控制台，用于统计平台运行数据、配置系统参数、上传更新客户端 APP 程序和配置平台菜单权限。运维管理控制台让移动终端安全管控平台具备高可用、动态化的运营运维能力，为企业 IT 管理员和租户平台运维服务提供了安全便捷的可持续运维的一体化工具。

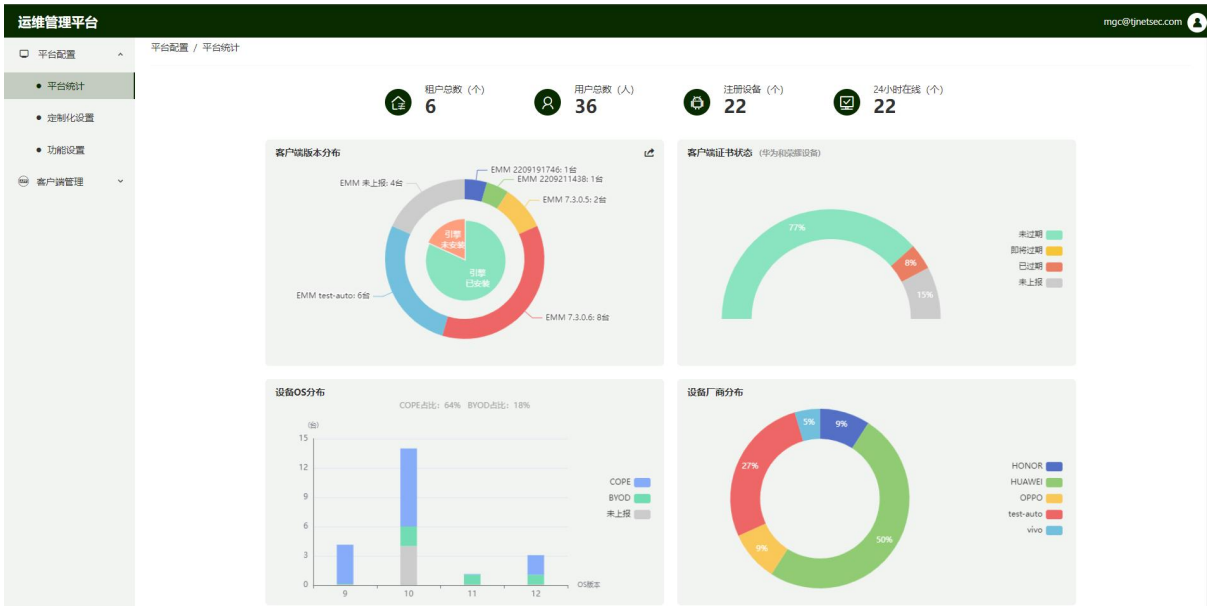


图 6.6：运维管理控制台

6.7. 移动安全态势感知

移动安全态势感知是以大数据分析技术为基础，从全局视角展示群体行为相关统计数据，包括概况统计，热门应用，交易分析，敏感词统计，日使用设备分布及违规用户分布等信息。

图 6.7：移动安全态势感知界面

6.8. 口令认证

为了平台信息安全，创建用户、修改密码和用户登录时，采用弱口令密码校验，增

加键盘排序及旁挂弱口令库校验等技术来防护用户口令安全。

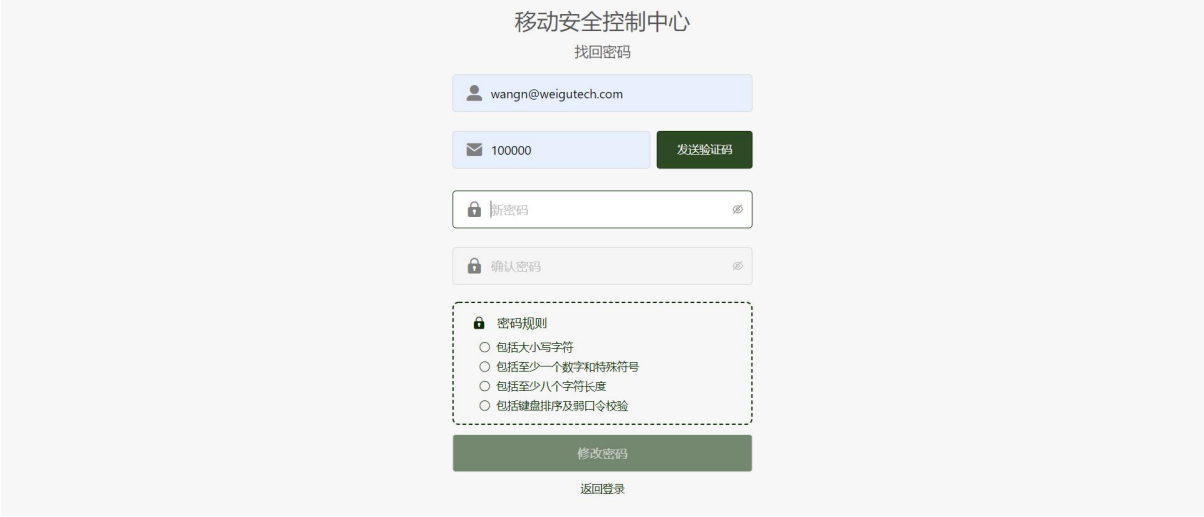


图 6.8：口令认证登录界面

6.9. 终端设备

支持的终端设备分为公版终端、适配终端与安全终端，公版终端选择范围较大，但管控力度较弱；适配终端功能较强，但可选范围相对小，可根据客户对移动安全管控的需求级别进行选择。

6.9.1. 公版终端

国产终端，Android 4.4 以上版本，不限制品牌型号。

6.9.2. 适配终端

国产终端，Android 4.4 以上版本，适配品牌为华为、荣耀、Oppo、一加、Vivo、小米、魅族主流品牌。

6.9.3. 安全终端

国产终端，选用经过安全加固的 Android 系统或国产操作系统，具备较强的管控能力。该安全终端是由各厂家为最终客户定制的 ROM 固定机型和型号的移动终端设备。

终端目录参加本方案附件，该目录定期更新，通过政企行业部门及时下发。

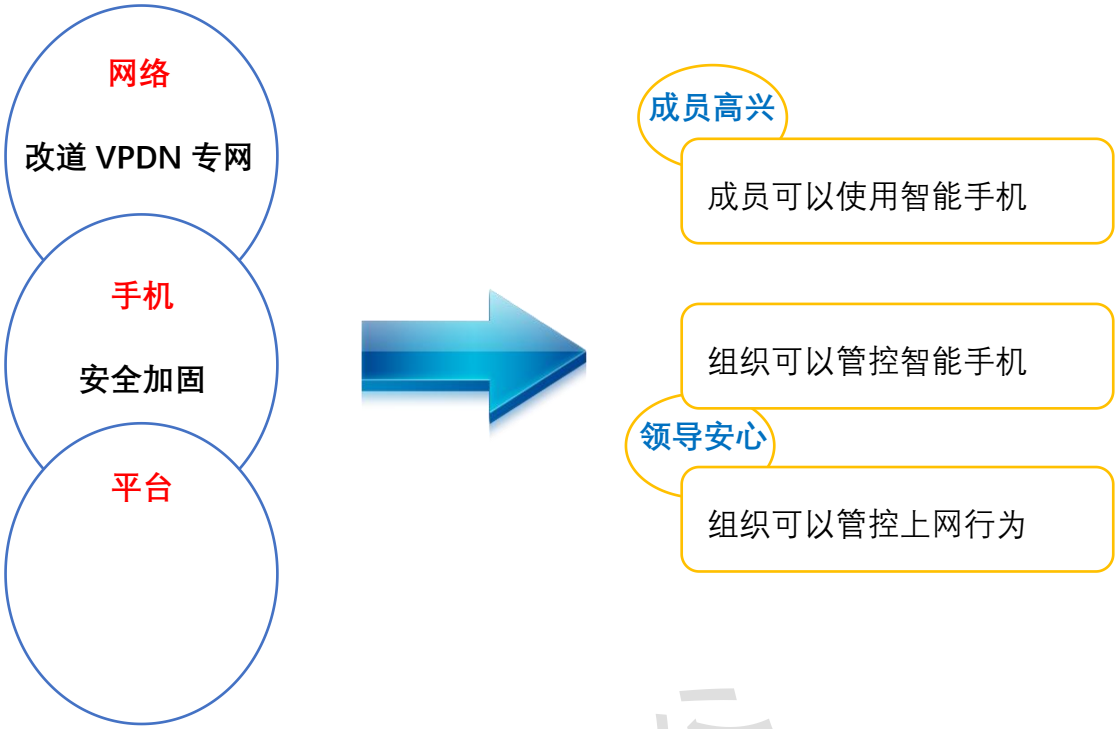
6.9.4. 公版终端与安全终端管控能力比对

管控项	华为公版	安全终端 3.1	VIVO 公版	OPPO 公版	安全终端 2.0	BYOD 其它设备
蓝牙	图标置灰					合规性检查动态关闭
WIFI	图标置灰				已连接的 WIFI 不断开，不让配置新 WIFI	合规性检查动态关闭
VPN	图标置灰且不可添加				不置灰，不可添加	不管控
移动热点	图标置灰				Android11 不允许手动操作	不管控
位置服务	图标置灰，点击提示	图标置灰（vivo 无效，已知问题）	图标置灰	图标置灰	图标置灰	不管控
外置存储	限制访问 SD 卡					不管控
USB 传输	不能通过 usb 连接手机					不管控

NFC	图标置灰				mate9 失效，已知问题	不管控
截屏	无法截屏	无法截屏，相关截屏选项置灰			不置灰，不可截屏	不管控
录音	无法使用系统录音机录音	无法使用系统录音机录音	可以使用系统录音机，但无声音	无法使用系统录音机录音	可以使用系统录音机，但无声音	不管控
摄像头	无法使用系统相机					
USB 调试	不能通过 adb 连接手机					不管控
恢复出厂	恢复出厂选项置灰	重置选项置灰	备份与重置选项置灰	恢复出厂选项隐藏	不置灰，不可恢复出厂	不管控
未知来源	每个应用的允许安装应用选项置灰且不可点击	设置可信安装源后，未知来源选项不对设置的电子市场干扰，同时文件管理器、adb 命令安装方式不可	每个应用的允许安装未知应用选项置灰且不可点击。	安装外部来源应用列表选项置灰。	不允许安装未知来源 app，未知来源不包括 adb 和特殊 app（应用商店等）。	不管控

		用。未设置可信电子市场不管控。管控参考华为	管控参考华为	管控参考华为		
OTG	不能使用该功能	OTG 连接选项置灰			不管控	不管控
飞行模式	图标置灰				Android11 不允许手动操作	不管控
黑名单 APP	不能运行，有相关提示	图标置灰，不能运行，有相关提示	图标置灰，不能运行	不能运行，有相关提示	图标置灰，不能运行	不管控

6.10. 产品特点与优势



✓ **上网行为管理**

- 多层次全面的终端安全能力，云-管-端的全方位安全保护；
- 全面的终端管控，支持公版终端与定制终端，客户根据安全需求进行选择；
- 多样灵活的上网策略管理与审计；

✓ **完全自主知识产权，符合国内合规需求**

移动终端安全管控平台由网安自主研发，具备完全的自主知识产权，满足国产软件合规需求。

✓ **防卸载防杀死，确保设备始终处于管控之下**

多项创新性技术，实现客户端防卸载和防被杀死进程，确保智能设备始终处在管控之下，不会脱离管控。

✓ **灵活强大的关键字过滤技术，无需对应用作任何处理**

创新的安全容器技术，不需要对微信/QQ 作任何处理，即可实现关键字过滤审计，以及禁用附近的人等社交功能。微信/QQ 可正常升级版本，升级后审计功能不受任何影响。

- ✓ **终端对国产 Android 手机适配率达 90%以上，主流品牌支持：华为、荣耀、Oppo、一咖、ViVo、小米、魅族等；（部分品牌终端仅支持项目批量采购）**
- ✓ **支持扩展国产密码，适配国产数据库、中间件和国产芯片服务器环境；**
- ✓ **高并发高可用性强，支撑过 30+万用户量 SaaS 平台；**
- ✓ **内置端到端加密、数据库加密、敏感数据脱敏、日志脱敏组件，符合国家网络安全法、数据安全法和个人信息保护法等法律法规的指导要求。**

7.产品价值

7.1. 安全合规

产品功能符合网络安全法、数据安全法和个人信息保护法等法律要求，遵循中国人民解放军内务条令（试行）、司法行政移动执法系统技术规范、电子政务移动办公系统安全技术规范和信息安全技术网络安全等级保护基本要求等行业标准，让企事业单位通过采用本平台打造基础的移动安全合规防线，为正常开展移动业务应用活动保驾护航。

7.2. 降本增效

为企业提供移动终端设备资产管理信息化工具，支持终端远程控制和追踪，有效防止终端硬件设备的丢失、损坏和保存在设备上的重要数据资产丢失、泄露，在保护企业的资产安全前提下，有效提高了企业对硬软件和数据的管理效率，降低企业人力管理维护移动终端设备的成本。

7.3. 安全防护

产品构建一体三面的安全防护体系，通过一个移动终端安全平台，实现终端设备从设备注册使用到日常管理、安全配置和最终淘汰注销的设备全生命周期安全防护体系；实现终端上移动应用从应用安装到应用管理、应用运行和最终应用卸载的应用全生命周期安全防护体系；实现终端上数据从生成收集到存储、使用、加工、传输、提供和公开的数据全生命周期安全防护体系。为企业提供移动终端的全生命周期硬软数三位一体的安全防护工具，有效保障企业的安全生产运营。

7.4. 行为规范

本平台利用固化的行业管控策略标准模板和管控流程，标准化管理终端设备的使用规范，从而直接影响用户的行为规范，让最终用户符合安全规范的指导要求，大大加强企业对最终用户的安全管理效率和效果。

7.5. 能力共享

本平台开放终端设备及其上应用和数据的管控能力访问接口，让周边安全关联系统和业务应用系统可以在充分授权的情况下调用到本平台的安全管控能力，实现安全管控一体化和业务功能的特色能力，比如业务系统可以和设备的地理及时间围栏管控能力进行联动，在设备进入到指定区域和时间段时启用或禁用某项系统功能，如拍照或录音等，从而实现个性化安全特性的业务应用功能；同时，本平台也可以提供用户设备的行为日志数据给安全大数据系统进行统一分析和关联预测，有效加强企业信息化安全的一体化态势感知和风险预测能力。

8.产品性能指标

8.1. 关键测试场景

- 5w 客户端以 5 个每秒速率注册激活(UserRegister&DeviceEnroll)，在 166 分钟完成注册，UserRegister 成功率 100%，DeviceEnroll 成功率 100%
- 5w 客户端以 50 个每秒速率重新连接(DeviceEnroll)，在 17 分钟完成注册，DeviceEnroll 成功率 100%
- 5w 客户端间隔 30 分钟接收 message 和 policy update，message 接收成功率 100%，policy update 成功率 100%
- EMM 系统资源占用平均 CPU:20%，MEM: 19GB，DB 系统资源占用平均 CPU:24%,MEM:11GB
- 全部 API 平均响应时间 100ms 内；

8.2. 产品性能结论

系统运行稳定，Sendmessage 和 PolicyUpdate 能够正常推送更新，能支持 5 万用户间隔 30 分钟上报微信、短信、通话记录，每秒上报 111 条数据，总计每天上报 960 万条数据。产品与同类产品相比，处于性能领先地位。

9.部署方案

9.1. 入驻式部署

移动安全管控平台支持私有化本地方式部署，平台部署在企业 DMZ 区内，通过 SSL 安全通道为移动终端提供设备管理、应用管理和安全推送等服务。同时，通过 VPN 客户端，实现合规移动终端对企业应用及企业敏感数据的安全访问。

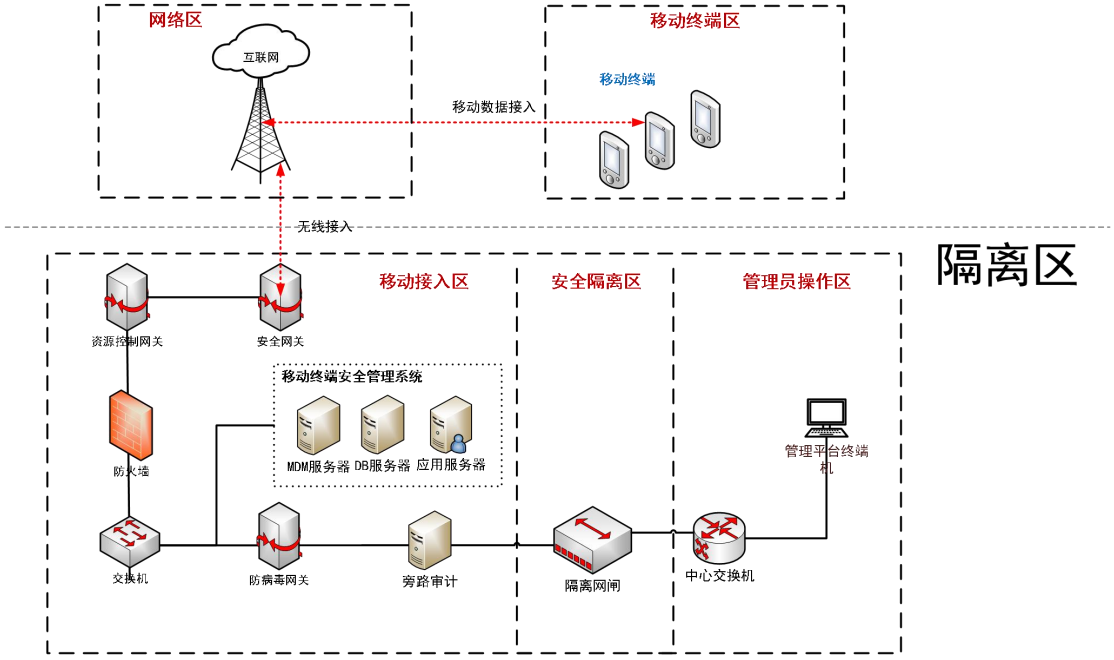


图 9.1-1：整体部署架构图

移动终端安全管控平台集群架构部署方案如下：

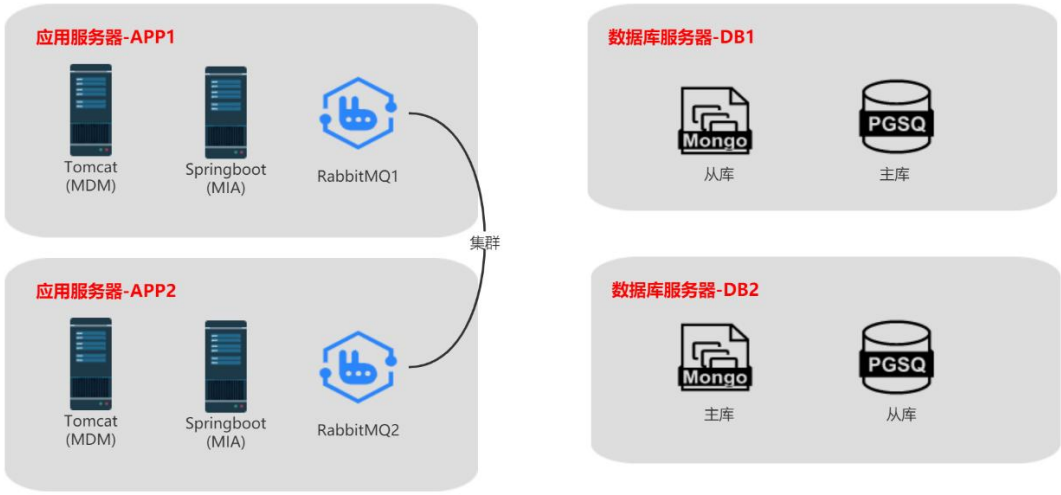


图 9.1-2：集群部署架构图

9.2. 云端部署

移动安全管控平台同时支持公有或私有云部署方式，针对云端部署，系统还支持多租户管理，租户间数据隔离，可支撑标准的 SaaS 服务模式运营。系统组件模块化，不同租户可选择不同模块提供服务。提供 MDM 云端租户管理平台，管理租户的开通及权限控制，基础应用下发等功能。

10. 售后服务

在产品保修期内，我司提供有限安装、问题调试、系统保修服务。

具体服务支持方式如下：

1）电话支持 （7×24 小时电话支持)

客户在使用本产品时如遇到问题，都可以从产品手册中得到电话支持方式，客户可以指定一名主要联系人及两名替补联系人与我司联系。一旦接到客户请求电话，我司技术人员将在规定时间内通过电话解决或回答客户的问题。

2）现场支持/现场值班（每周一至周五 9:00-18:00)

对于通过电话和远程处理都无法解决的问题，我司将派出工程师到客户现场为客户提供现场产品调试服务，保证产品在用户网络上正常运行。保修期后本服务需要另行收费，具体的收费标准可与我司协商决定。

3）有限安装服务

由于本系统涉及到较多的网络知识和安全知识，如果客户无法自行安装、配置购买的本产品，我司可以派出工程师到用户现场为客户提供现场产品安装服务。保修期后本服务需要另行收费，具体的收费标准可与我司协商决定。

4）保驾服务

为了保证客户购买的本产品长期正常运转，如客户需要时，我司可以安排工程师对产品及客户的产品进行定期巡检服务，包括定期回访、系统检测。保驾服务需要另行收费，具体的收费标准可与我司协商决定。

11. 典型案例

客户	项目情况	项目特点
江西省强	1.集成网安卫谷的安全移动办公系列产品； 2.支持设备生命周期中全部 22 个安全需求点管控； 3.为用户提供可管可控的移动安全终端；	1. 率先实现了基于国产双操作系统的司法监狱移动信息化管理解决方案； 2.终端外设强管控，超过三星、苹果、黑莓、阿里现有 OS；

戒所	4.基于国产操作系统，集成及开发众多移动办公应用，包括主流 OA 系统、云拍照、云视频、云录音、及时通信、对讲、一键报警等。	3.与客户现有的门禁系统平滑对接； 4.生活模式、工作模式、执勤模式按需灵活切换。
潍柴集团	1.为潍柴集团全国 30 余处驻外服务站提供工作终端管理系统 2.网安卫谷提供便捷的移动终端定位巡视服务 3.个性多样化的分析审计功能，便于潍柴集团管理人员了解全国各地服务站工作终端的使用情况。	1 提供深度定制化的国产终端； 2.与潍柴集团服务系统，身份管理系统等集成对接，实现集团内服务站人员信息的安全管理； 3.系统深度定制化服务，实现集团内用户、管控、审计等全方位便捷服务。
绿色军营	1. 网安卫谷提供智能移动终端安全管控整体解决方案和产品的持续升级迭代服务； 2. 运营商提供移动终端、服务器和网络接入、防火墙设置及后期运维； 3.网安卫谷提供专家级运维服务、技术咨询和指导。	1.多层次全面的终端安全能力，云-管-端的全方位安全保障； 2.公版终端与定制终端的全面管控，客户可根据安全需求定制； 3.多样灵活的上网策略管理与审计。