多信云

多信云安全移动办公

(Safe Mobile Workforce)

技术白皮书

厦门多信云科技有限公司

目 录

前　言

习近平曾指出，世界经济数字化转型是大势所趋。在企业数字化转型升级浪潮下，移动办公凭借高效、便捷等优势，成为新的办公潮流。移动办公为企业生产效率的提升带来巨大红利，利用智能手机、平板电脑进行信息收发、流程审批、文件传输及远程协作等工作，能够显著提升企业办公效率。疫情深刻改变了人们的生活及工作方式，更加速了移动办公的普及。后疫情时代，由于移动办公习惯已经养成，移动办公、远程协作趋于常态化。

但是，移动办公在带来工作效率提升的同时，也存在前所未有的信息安全风险。政府、企业的机密资料，随移动终端在互联网环境下流转，无论是员工主动泄密或因设备丢失、被攻击造成的被动泄密，都会造成严重损失。而对于银行、证券等金融行业和政府、军队等国家机构而言，信息安全更关系到国家安全。

云计算、5G、虚拟化等新兴技术催生了云办公，为解决移动办公的信息安全问题提供了新的思路。2021 年 1 月 19 日，中国科学院邬贺铨院士在 2020 科技风云榜上指出，“通过云化、虚拟化、互联网等多种模式相结合，5G 将引领网络技术整体创新”、“依托 5G 网络，终端的计算将向云端迁移，终端不需要下载核心软件，降低了终端的成本，能够实现即插即用”。

厦门多信云科技有限公司是华为公司战略合作伙伴，依托云计算、虚拟化等技术，推出多信云安全移动办公解决方案，为企业解决信息安全问题提供了全新路径，能够有效帮助企业解决移动办公场景下的信息安全问题，助力企业实现数字化转型升级。

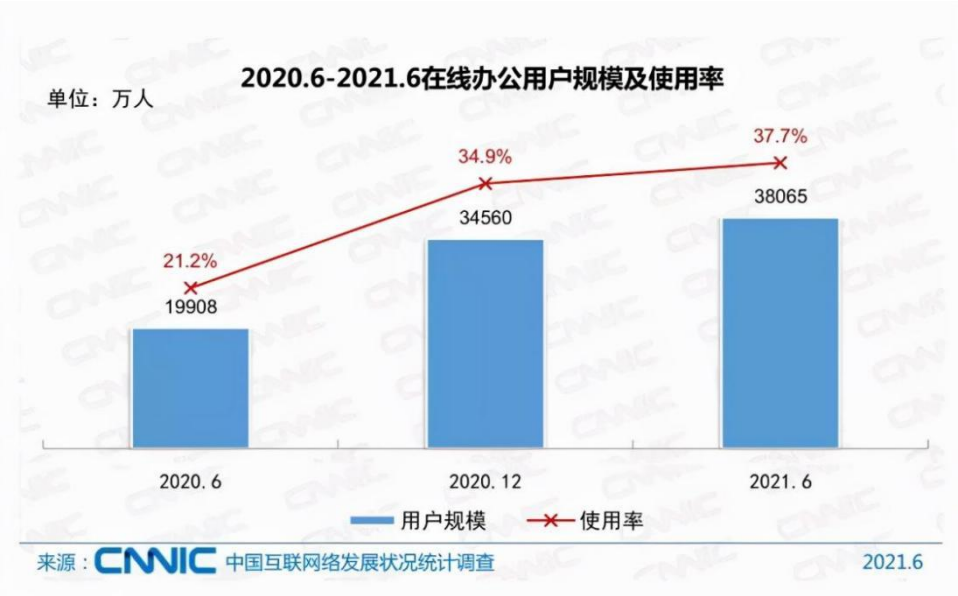
第一章 传统移动办公模式面临数据安全隐患

1.1 数字化转型浪潮下，移动办公成为趋势

随着我国数字经济规模逐渐扩大，以及移动互联网、人工智能、大数据等技术的不断渗透，企业数字化转型进程加快。尤其是经历疫情的洗礼，驱动企业以前所未有的速度和规模拥抱新的变革。数字经济呼吁一种更为高效和灵活的办公方式，而移动办公无疑是企业数字化转型最基础、最核心的工具。

移动办公并不单指远程办公，广义上凡是使用移动终端（智能手机、ipad 及笔记本电脑等），不受时间、地点、网络限制，能够随时随地处理与业务相关的工作都属于移动办公范畴。对于企业而言，移动办公不仅能提升办公效率，而且能延伸企业服务网络，拓宽服务渠道及业务覆盖面。凭借便捷、高效等特点，移动办公深受人们青睐。

相关研究及统计数据，均印证了移动办公趋势的确定性。据中国互联网络信息中心调查报告显示，2020 年春节期间，我国有超过 1800 万家企业采用了线上远程办公模式。2020 年 6 月，我国远程办公用户规模达 1.99 亿，占网民整体的 21.2%。到 2021 年 6 月，我国在线办公用户规模攀升至 3.81 亿，网民使用率为 37.7%。



2021 年 11 月 2 日，国内移动互联网大数据公司 QuestMobile 发布《2021 中国移动互联网秋季大报告》。报告显示，在线办公的用户数量和市场规模显著提升。截至 2021 年 9 月，中国移动互联网月活用户达到 11.67 亿，其中办公商务类 APP 用户数量达到 6.19 亿人，同比增长 8.2%，活跃渗透率达到 53.0%。

Source：QuestMobile TRUTH 中国移动互联网数据库 2021年9月

根据艾媒咨询数据报告显示，自 2017 年以来，我国智能移动办公市场规模成稳步上升趋势。2020 年智能移动办公市场规模达到 375 亿元，预计 2021 年中国智能移动办公市场规模将达 469 亿元。

1.2 企业移动办公转型，数据安全问题凸显

在移动办公趋势下，企业在享受移动办公便利的同时也面临着严重的信息安全及数据安全挑战。移动办公设备一旦丢失，则可能沦为黑客攻击企业网络的利器。而员工的智能手机、平板、电脑等私人设备大量接入企业内部系统，对企业的信息安全构成重大挑战，企业面临严重的信息泄露风险和隐患，尤其是金融、保险、证券、政府、军队，以及其他对数据安全要求较高的企事业单位。

中国信通院、普华永道、平安金融安全研究院联合发布的《2018-2019 年度金融科技安全分析报告》数据显示，44%的金融机构均遭遇过不同程度的信息泄露。根据 IBM Security《2021 年数据泄露成本报告》显示，2021 年，企业平均每起数据泄露事件成为 424 万美元，是自 2004 年以来的最高值，远程工作是导致数据泄露成本提升的主要原因。

远程沟通过程中，聊天内容往往会涉及到产品设计资料、内部营销规划、招投标书文件、客户信息、合同协议等重要数据，如何保障它们不被窃取、泄露？员工离职或者设备丢失后是否会造成数据泄露？怎样减少管理移动端的费用以及难度？员工的隐私如何保护？这是企业移动办公战略落地的主要风险和顾虑所在。

1.2.1 企业移动办公场景的数据风险

员工用于办公的移动终端，主要包括企业配发设备及员工自带设备两种，这两种模式均存在不同程度的信息安全风险，具体如下表所示：

表 1-1 企业配发的移动终端面临的主要信息安全风险

风险类别	具体说明
设备遗失风险	该部分设备中包含企业专有的开发应用和数据，一旦遗失将会造成涉密资料泄露，导致不可预估的严重后果。
移动系统安全风险	在企业配发的设备上安装其他应用，或将设备越狱后，可能会导致外部应用与企业内部应用产生兼容性问题，甚至造成数据泄露。
设备资产管理风险	该部分设备属于企业资产，需要收集资产相关的信息，不适合安装或使用其他应用（如：微信、微博及游戏等）。
移动应用发布风险	外部的 App Store 中大量应用有安全隐患，并且缺乏严格的安全检测机制，如果把电子政务网中的应用放置在外部的 App Store 中可能会出现被仿冒、破解等安全隐患。自主开发的应用需要通过企业内部的 App Store 进行分发推送。

表 1-2 员工使用自带移动终端面临的主要信息安全风险

风险类别	具体说明
内部涉密信息泄露风险	企业为防止机密信息泄露，通常会通过相关软件和制度进行管控，如：限制 PC 外设、数据泄露系统控制、制度控制等，但是传统的控制手段无法对智能设备进行控制，智能设备可连接电子政务网络获取资源，通过拍照、摄像、录音等方式获取企业敏感信息。
数据遗失风险	调查研究发现，多数智能设备使用者会将自己的个人信息和资料存放在智能设备中，设备一旦遗失，个人的相关信息、手机电话本、备份资料等，有可能落入他人之手。
病毒感染风险	智能终端同样存在病毒问题，病毒会对移动终端的系统和应用造成影响，而传统的防病毒软件无法对其进行防护和管理，一旦设备在外面感染病毒，可能会传播到内部网络中。
移动应用风险	外部的 App Store 中大量应用有安全隐患，并且缺乏相应的安全检测机制，放任员工自由安装，很可能导致应用程序的风险带入到内部网。企业需要搭建内部 APP Store 来下发自主开发的 APP 应用，同时管理控制移动设备上安装的应用。

1.2.2 移动应用开发过程的风险

随着移动智能终端的普及，越来越多的企业将其 IT 业务系统从传统 PC 模式向移动终端模式迁移。企业在快速开发和推广 APP 应用系统的同时，不可避免地引入了大量新的安全问题，如用户敏感信息泄露以及企业内部网络被渗透等。

Category	2013	2014
M1	Insecure Data Storage	2013 M2 + 2013 M10
M2	Weak Server Side Controls	2013 M1
M3	Insufficient Transport Layer Protection	2013 M3
M4	Client Side Injection	2013 M8 + 2013 M10
M5	Poor Authorization and Authentication	2013 M5
M6	Improper Session Handling	2013 M9
M7	Security Decisions via Untrusted Input	2013 M4
M8	Side Channel Data Leakage	2013 M7
M9	Broken Cryptography	2013 M6
M10	Sensitive Information Disclosure	Lack of Binary Protections

1.弱服务器端控件

在 OWASP 排第一的漏洞是“脆弱的服务器端控件”，简言之，即没有使用安全的方式从移动应用程序向服务器端发送数据，或在发送数据时暴露了一些敏感的 API（Application Programming Interface，应用程序接口）。例如，在对 Android 应用程序登录服务器的凭据进行身份验证时，没有对输入进行验证。攻击者可修改凭证以获得服务器敏感或未经授权的区域权限。这是移动应用以及 Web 应用都存在的漏洞。

2.不安全的数据存储

在设备上存储任意用户均可访问且与应用直接相关的信息。大量安卓（Android）应用在 Shared preferences，SQLite（以明文形式）或外部存储器中存储机密的用户信息或应用程序信息，开发者即使把敏感信息存储在/data/data/package-name 目录中，但是只要手机被 Root，就会被恶意应用或攻击者访问。

3.传输层保护不足

许多 Android 开发者使用不安全的方式进行数据传输，比如以 HTTP 的方式，或者没有正确实现 SSL（网络加密传输协议）。这使得应用程序在网络上容易受到各种不同类型的攻击，例如，在应用向服务器发送数据的时候进行数据包拦截、参数操作、修改响应数据，以获得应用锁定区域的访问权限。

4. 意外的数据泄露

当应用程序存储数据的位置本身脆弱时，容易造成意外的数据泄露。这些位置可能包括剪贴板，URL 缓存，浏览器的 Cookies，HTML5 数据存储，分析数据等等。例如，一个用户在登录银行应用的时候已经把密码复制到了剪贴板，恶意应用程序通过访问用户剪贴板数据就可以获取密码。

5. 弱授权和身份认证

安卓应用程序在没有适当安全措施的情况下，通过客户端检测进行用户验证或授权，就会存在风险。应当指出的是，手机 Root 后大多数客户端的保护都是可以绕过的。因此，建议应用程序开发者使用适当的检测方法在服务器端进行身份验证和授权，然后在移动设备上使用一个随机生成的令牌来验证用户。

6. 密码破解

使用不安全的加密函数来加密数据组件，其中可能使用了已知的脆弱算法，如 MD5、SHA1、RC2，甚至没有采取安全措施定制开发的算法。

7.客户端注入

SQL 注入：run app.provider.query [Content Provider URI] --projection "* FROM SQLITE_MASTER WHERE type='table';- -"

8.通过不可信输入进行安全决策

在移动应用程序中，开发者应清洗和检验用户输入或其它相关输入，不可信的输入可能导致应用安全风险，如客户端注入。

9.Session 会话处理不当

在进行一个移动应用的 session 处理时，开发者需要关注很多的因素，比如适当过期的有效身份验证 cookie，安全令牌创建，cookie 生成和旋转，以及后台失败的无效 session。在 Web 应用和 Android 应用程序之间必须保持一个适当的安全同步。

10.缺乏二进制文件保护

不能够有效阻止应用程序被逆向或者反编译。Apktool、dex2jar 等工具可以对 Android 应用进行逆向，从而使应用暴露出各种安全风险。为了防止应用被逆向，开发者可使用 proguardand 和 dasho 等对应用进行加固。

1.3 5G 云办公助力解决移动办公信息安全问题

5G 时代网络传输速率将达到 10GMpbs，将是 4G 峰值的 100 倍，时延将降低到 1 毫秒（千分之一秒），5G 网络成为未来数字社会的驱动者。5G 技术将使传统的通信，向人与人、人与物、物与物的实时连接方向演进，革命性的技术突破，将重塑经济业态和社会关系。5G 也将带来全新的办公体验，云办公正是 5G 重要的应用方向。

表 1-3 移动通信技术与典型应用场景

技术阶段	业务类型	主要应用场景举例
1G	模拟语音	手提电话（仅支持语音通话功能，俗称大哥大）
2G	数字语音	短信
3G	移动互联	智能手机、电子商务、微博、微信
4G	数据通信	视频、短视频
5G	万物互联	云办公、超高清视频、云游戏、AR/VR、自动驾驶、远程医疗、工业互联网、智能家居等

资料来源：张勇敢,章伟飞,张森洪.1～6G 移动通信系统发展综述；李炜炜,袁军.融合视角下媒介素养演进研究：从 1G 到 5G.

2019 年 6 月，工信部向四大运营商发放 5G 商用牌照，正式开启 5G 商用进程。2020 年政府出台以 5G 为基石的新基建刺激计划，“新基建”被写入当年《政府工作报告》，此后我国 5G 建设开始大规模提速。根据国家网信办《数字中国发展报告（2020 年）》，我国 5G 网络建设速度以及规模均位居全球第一，5G 专利数量也位居全球第一。根据工信部统计数据，截止 2021 年 8 月底，我国 5G 基站数量已经超过 100 万个，占全球 70%以上，5G 终端连接数超过 4 亿个。

根据《阿里巴巴新基建洞察之 5G 智能经济应用场景研究报告》，云端一体、视觉锐化、体验极致和现场增强被视为 5G 四个主要应用趋势。在 5G 网络及云计算的支撑下，终端算力向云端转移成为了可能，原本需要实体终端完成的计算，依托 5G 网络可交给云端完成，终端设备只需要一块屏幕及网络即可使用，因此云端一体、端云协同将成为 5G 时代的显著趋势。

5G 网络拥有大带宽、低延迟、高可靠、广连接等优势，并具有云化、虚拟化、网络切片等特点。在云办公模式下，企业的移动办公应用全部部署、运行在云端服务器内，员工在屏幕上远程操控，由于数据不落地，将具有高度安全性。依托 5G、云计算及虚拟化等新兴技术，厦门多信云科技有限公司致力于为企业提供高度安全的移动办公解决方案。本方案可以解决企业移动办公过程中面临数据安全问题及相关挑战，具体如下：

1、确保业务数据安全。在传统移动应用架构下，业务数据存放在智能终端的存储中。一旦发生恶意代码感染、手机丢失或内部员工故意泄露信息等情况，存放在智能终端的数据将不受保护。虚拟移动架构把所有涉及业务的数据存放在云端服务器，智能终端不存储任何敏感数据。即使发生极端情况，也不会发生数据泄密，能够有效确保业务数据安全。

2、无线访问的安全。原有架构只能通过用户认证及运营商保障的方式，确保访问安全。移动云计算模式可以解决端到端的访问安全，通过远程智能终端虚拟桌面的用户账号安全措施、访问通道加密、后端应用边界安全防护等技术，确保后端数据访问全程安全可靠。

3、更简便快捷的应用发布及管理。原有架构，每一个新移动应用发布时，均需要终端用户重新安装 APP，推广一次涉及数千智能终端，成本高昂。本方案中的技术，可在后端虚拟智能终端桌面统一发布应用，用户只需打开该远程桌面，即可快速使

用，无需安装。

4、支持使用自带设备安全办公，节约设备配发成本。用自己的手机办公是发展趋势，每个员工都有 1-2 台自有智能终端。相对于企业下发工作手机，员工使用自有手机安装企业办公应用，可节省大量成本。但是，由于大部分员工不愿意将单位的应用安装在自己的手机上，导致 BYOD（用自带设备办公）无法推广。借助移动云计算模式，可区分企业与员工私有的应用，员工仅需打开远程虚拟手机桌面，即可使用各种移动应用，不需要在实体手机上再次下载，不占本机内存，有效隔离公私数据。

此外，采用移动云计算模式，用户可以更快捷地开展移动应用的开发及使用，各种应用的部署无需再考虑数据安全、部署成本的问题，通过此平台可快速将应用发布到全网智能终端上。

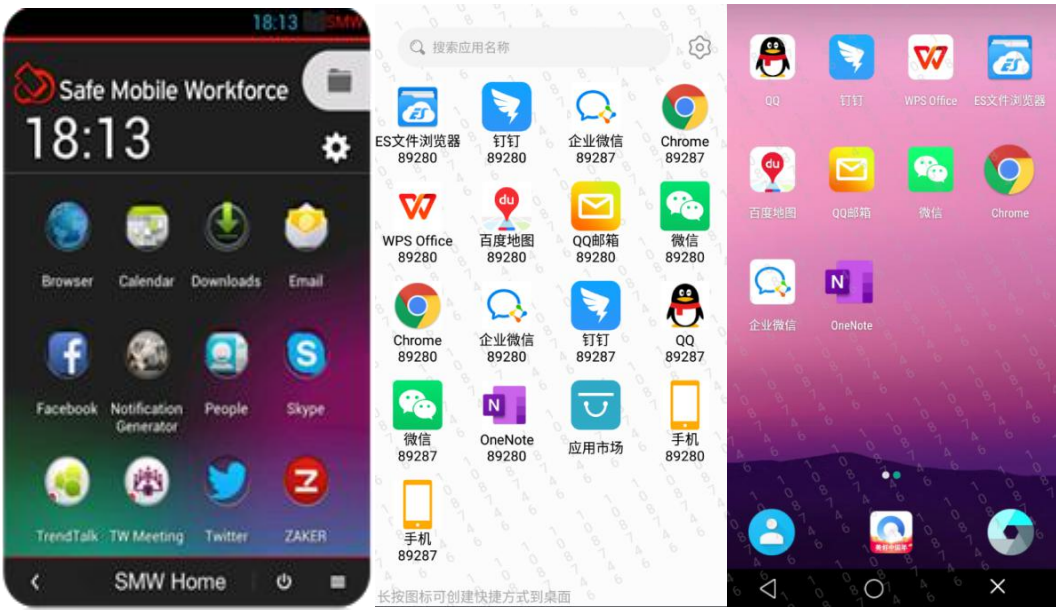
第二章 多信云安全移动办公解决方案

2.1 多信云安全移动办公解决方案简介

1.多信云终端简介

多信云终端是采用世界领先的虚拟移动基础架构（VMI）及云计算技术研发的安全移动办公解决方案，能够为用户创建高度安全的虚拟工作空间。用户工作区基于安卓（Android）操作系统，用户通过安卓移动设备上多信云终端应用程序即可访问。用户点击多信云终端应用程序，即可打开全新的手机界面，获取企业定制化的移动应用程序和数据，这些应用及数据不离开数据中心，从而确保数据的高度安全性。

简而言之，多信云终端依托“从云到屏”的技术，企业办公应用安装、运行在企业自己的云端服务器内，用户通过手机界面操作办公虚拟手机，操作指令和运算结果在屏幕和云端来回实时传输，在5G高速网络下拥有极低的延迟，能够媲美实体手机的操作体验。多信云终端兼容安卓应用，具备实体手机的性能和操作体验，因此能够在保障数据安全的同时，确保移动体验。



2.多信云终端的主要特点

（1）适配Ios、安卓及Windos设备

多信云终端采用虚拟化技术，能够虚拟出不同配置的移动办公手机。而且虚拟办公手机拥有和实体手机一样的性能及操作体验，能够适配市面上主流Iso、Android、Windos等移动设备。

（2）架构安全，带来信息安全

多信云终端能够依托集中化的服务器虚拟移动操作系统，并通过高效的远程显示协议实现网络访问和操作。由于所有虚拟办公手机都托管在企业的云服务器上，并由管理员进行维护，因此多信云终端能够明确区分可供用户使用的个人数据和企业数据，确保数据安全，并提供更为集中、有效的工作区，方便企业在后台进行管理和维护。

图2-1 Safe Mobile Wordfoce架构说明

2.2 多信云安全移动办公解决方案主要功能

（1）移动业务数据保护

企业所有应用程序和数据保存在公司服务器上，由公司管理员控制。

（2）简化的移动管理

用户可从任何移动设备访问其工作区，网络管理员可以通过Web控制台远程管理所有工作区。

（3）保障移动用户体验

多信云终端支持Android移动操作系统，提供原始的移动用户体验。多信云终端附带高级渲染引擎，能够为智能手机和平板电脑提供熟悉的移动用户体验。

（4）可以集成企业私有云存储服务

多信云安全移动办公解决方案提供私有云存储服务，让企业管理和同步文档更加高效、便捷。

（5）支持主流身份认证方式

多信云终端支持市面上的主流身份认证方式，便于进行用户管理。多信云终端的技术核心是Linux的“容器”技术。Linux的“容器”技术，能够支持用户将某些关键的应用打包在“容器”中。本项目基于“容器”技术，把智能终端操作系统及应用打包在“容器”中，然后通过加密通道，发布到所有智能终端。多信云终端的用户按照分组类别，在登录虚拟手机桌面后，即可访问各自定制的手机桌面及应用。

2.3 多信云安全移动办公解决方案主要优势

1.业务数据不落地

在各自的虚拟手机桌面中，终端用户的实体手机不能访问及存储虚拟手机桌面的数据，但虚拟手机桌面可以调用终端智能手机的各种外设，如摄像头、无线网卡等。因此，虚拟手机桌面既能实现终端手机各种功能，同时不用担心业务数据存放到智能终端的存储中。即使发生手机丢失、感染恶意代码、甚至是内部员工泄密等极端情况，也能确保业务关键数据不会泄露。

2.保障移动业务通讯及用户访问的安全性、可靠性

端到端访问加密，从智能终端到电信运营商边界、从电信运营商边界到后端移动安全办公平台、从管理员到移动安全办公平台均为SSL加密，不存在网络窃听风险。外网用户登录，必须通过中间安全隔离层访问，并且同时通过动态密钥、用户认证等方式，来确保登录的安全性。

3.提供多用户移动云桌面服务

如何通过后端服务器建立多个并行的虚拟智能终端桌面？

目前市面上所有的技术仅支持通过后端提供多个虚拟PC桌面（如Windows），尚无技术可以支持通过后端计算资源提供多个虚拟智能终端桌面（Android、IOS），利用虚拟化技术实现将是最佳方向。目前Linux具备虚拟化技术及“容器”技术，通

过“容器”技术，可以在容器中封装各种不同的智能终端操作系统。通过虚拟化技术，可实现在特定计算资源中，同时运行多个智能终端。

4. 确保在无线网络环境的访问安全

大部分智能终端，均需通过3G/4G网络访问电信运营商后端系统。如何确保用户身份合法性，访问通道的安全性是一个挑战。访问身份的合法性，可通过目前比较成熟的动态密钥方式+用户身份认证方式解决。通过动态密钥及静态密码等双重方式的保障，可确保访问者的身份唯一性，同时无需担心密码被盗的风险。

访问通道安全性，可以通过建立安全访问中继的方式解决。除了在访问通道进行加密以及边界防护外，还可以加入类似移动终端访问中继的方式，提升内部数据访问的安全性。

表 2-1 多信云移动云计算方案对比传统移动安全方案的优势对比表

比较项目	传统移动安全方案（MDM）	新型移动云计算方案（VMI）
数据安全	移动应用需要在手机上安装，必然会存在缓存，有数据泄露风险。	数据不落地，移动应用在云端发布及运行，手机本地完全没有应用数据，应用数据不出数据中心。
应用安全	由于移动应用需要安装在手机中，存在被破解的风险。黑客容易通过 APP 逆向分析，找到应用中的漏洞，从而发起攻击，导致数据外泄。	移动应用部署在云端服务器，不部署在手机端，因此黑客难以获取手机应用程序，无法进行逆向分析，保障了企业数据安全。
移动应用开发	对于不同移动系统需要开发不同的 APP。开发一个移动应用往往需要支持 Android、iOS、Windows 三种主流操作系统，开发成本较高。	只需要开发 Android 应用，就可以在 VMI 中进行发布，大幅度降低了开发难度及开发成本。
移动应用屏幕适配	大量不同大小屏幕及分辨率的手机，造成移动应用开发过程需要大量的适配测试。每种新手机推出时，应用开发商就需要进行应用适配测试，造成大量开发测试工作，购买新手机导致成本上升。	VMI 手机客户程序能提供屏幕适配功能，因此应用开发商不需要对每款手机进行测试，而只需要依赖 VMI 手机客户端自动检测手机型号及屏幕分辨率来实现屏幕适配，满足用户体验，大幅度降低开发成本。

移动应用分发方式	移动应用需要推送到手机端，因此手机用户需要进行安装，大量及高频度的移动应用推送，将会影响到手机性能和带电时间，直接影响用户体验及应用可用性，导致用户主动卸载应用。	由于在云端虚拟移动应用，因此不需要向手机推送应用，只需要在虚拟机中部署应用即可；用户通过客户端程序直接访问虚拟机来获取应用，不需要安装及更新应用；云端移动应用不会消耗用户手机的存储、CPU 和电池，对用户手机配置要求较低，能适配各种系统。
移动应用运维管理	需要通过大量的定制策略来控制移动终端及应用。不仅要进行终端安全管理，同时还要进行应用的分发及更新，要追踪每一个用户是否成功部署移动应用，如果没有成功部署还需要进行技术支持。同时终端的安全也影响到企业数据安全，因此需要投入大量的精力进行安全管理。	运维只需要管理虚拟机，应用分发只涉及虚拟机的应用资源池配置，不涉及终端用户，分发过程只有几秒钟。然而，传统 MDM 的分发过程需要长达数天，同时存在大量推送失败的情况，VMI 的应用分发高度集约且速度极快。另外，VMI 数据不落地，管理员无需关心一般用户的移动终端安全，不需要花费大量精力对个人用户的移动终端进行管理和支持。
数据擦除	MDM 的数据擦除依赖网络通信，一旦手机终端被偷或遗失。小偷或捡到手机的人第一时间拔掉电池或 Sim 卡，手机无法接受到无线信号就无法获取远程擦除指令，实际该功能就没有实现可能。	由于用户数据都存在云端，一旦用户手机被偷或遗失，只要密码没有外泄，数据就不会外泄。用户如需擦除数据，也只需要管理员对虚拟机下发擦除指令，瞬间即可擦除，不依赖用户手机的网络连接。
个人隐私保护	MDM 需要获取大量终端信息，用户会担心泄露个人隐私。	VMI 不需要监控终端状态，不获取涉及用户隐私的数据。

5.有效防止上班“摸鱼”

办公留痕，方便绩效考核：依托数据云端存储特点，多信云移动办公能够实现办公留痕。例如，对员工与客户的微信交流记录、项目在线洽谈记录、客服处理用户咨询的数量及过程等进行留痕。根据后台数据，既能帮助管理人员及时了解下属工作进度及任务完成情况，也可以作为企业考核依据，在一定程度上预防“摸鱼”。

设置应用白名单：在多信云管理后台，管理员可设定应用白名单，禁止员工安

装违规应用，防止员工在办公界面从事与工作无关的内容。

自动录制办公操作轨迹：职员打开虚拟移动办公界面后，所有操作轨迹后台自动录制。企业管理员可在后台设置按间隔时间自动截屏，或录制操作轨迹视频。员工移动办公的画面截屏及视频，管理员可在后台回放、查看。

2.4 多信云移动安全办公解决方案应用场景

多信云终端致力于解决办公领域的数据安全问题，能够针对政府、企事业单位不同场景的移动办公需求进行定制化开发，满足差异化需求。

1.政务办公场景：解决数字政务落地安全风险

伴随着政府数字化转型升级、政务上云成为大趋势，各地政府对于数字政务安全的重视程度只增不减。在政府办公领域，多信云终端能够保障接入安全，结合政务移动数据的集中存储机制，有效防范移动数据外泄和违规外联，虚拟办公手机统一云端部署，数据不落地，防破解、防入侵；内外网隔离，有效隔离公私数据；应用统一安装；操作轨迹自动录制，能够有效解决数字政务落地的安全风险。

2.企事业单位办公场景：确保机密信息及数据安全

多信云终端能够有效隔离公私数据，让工作和生活互不干扰。而且，虚拟工作手机上的客户沟通信息全部保存在云端，方便职员离职交接，避免客户信息泄露。在企业办公领域，多信云终端能够广泛应用于银行、保险、证券等金融机构，以及对数据安全要求较高的企事业单位。

例如：

（1）金融：多信云移动安全办公为金融单位提供一个统一的移动运营管理平台，保障金融单位的员工移动办公安全以及业务员移动办理业务的安全。

（2）教育：多信云移动安全办公可大幅度降低学校移动运维工作量，并支持移动教学备课跨平台资源共享，打造新型信息化教育模式。

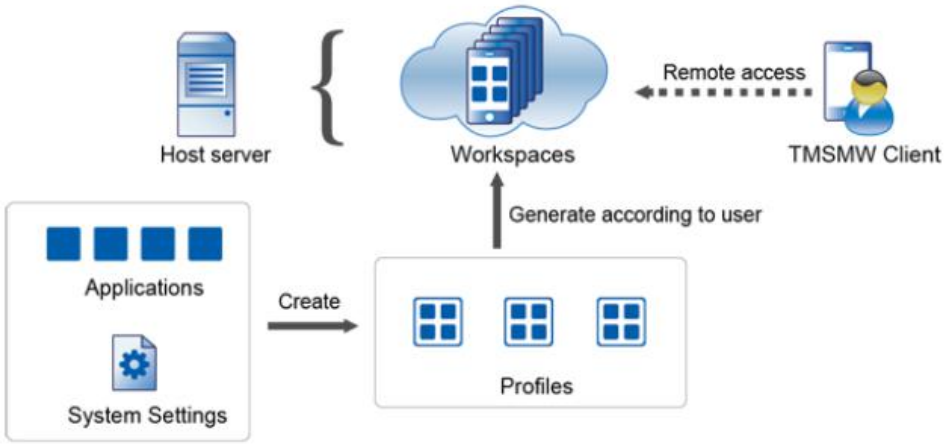
（3）医院:多信云移动安全办公为医疗提供医生值班轮岗解决方案，能够避免医生真实手机号泄露，患者沟通数据全部保存在云端服务器，方便医生轮岗及值班。采用虚拟手机沟通，能够确保医患及时沟通。

第三章 多信云虚拟移动基础架构

3.1 虚拟移动基础架构介绍

多信云安全移动办公解决方案采用全球领先的虚拟移动基础架构（Virtual Mobi-le Infrastructure，简称：VMI），VMI 是在用户内网安全机房中的 ARM 服务器上创建 Android 虚拟机，用户手机通过网络连接虚拟服务器，进而实现移动桌面传输及操控。IT 管理员能够通过管理界面，为用户创建、启动、停止、删除虚拟手机，并发布移动应用。由于 Android 虚拟机比 PC 虚拟机镜像小，载入速度很快。

移动终端与虚拟机之间的“互动”，则借助远程移动桌面协议，即实现虚拟机屏幕传输到移动终端，而移动终端上触摸信号则从移动终端传输到虚拟机。企业用户可通过 Android 或 iOS 移动设备上安装的客户端程序访问。使用客户端程序，用户可以获取依据业务定制化的移动应用程序和数据，而这些应用及数据不离开数据中心，从而确保数据的高度安全性。

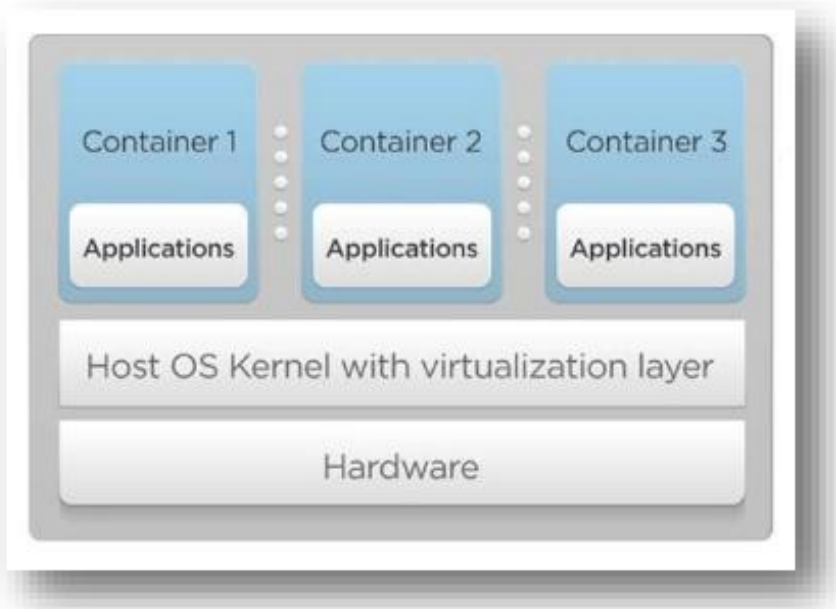


如上图所示，Host Server 作为主虚拟服务器包含了所有的用户虚拟机、APP 应用，当用户远程请求获取虚拟移动桌面时，Host Server 依据每一位用户的账号对应的配置文件（Profiles）来创建移动办公空间（Workspaces），用户就能快速进入安全移动虚拟终端，从而得到移动应用服务。

3.2 MIC SMW系统运行逻辑

每一个容器包含了 Android 实例，并且可以管理虚拟安卓系统。只有当用户登录 MIC SMW 系统时，对应该用户的 Android 实例才会在容器中生成。每一个用户拥有自己独立的虚拟安卓系统。移动设备通过 RMX（远程移动体验协议，该协议为多信云科技专利技术）获取虚拟安卓系统桌面影像。MIC SMW 客户端采用 RMX 协议来显示远程虚拟移动桌面。以下为 RMX 协议的描述：

- RMX (Remote Mobile eXperience) 是优化过的远程访问协议，同时支持 iOS 和 Android 移动系统。
- RMX 可以智能采用不同的数据编码方式，以适应不同的网络环境及移动终端配置。



3.3 多信云安全移动办公集中管理

多信云科技研发的安全移动办公解决方案——Safe Mobile Workforce 采用 C/S 结构，管理员通过浏览器即可对企业所有的虚拟办公手机进行管控，SMW 服务器支持管控虚拟平台中用户对应虚拟机的配置，包括程序策略下发，状态检测、风险监控等功能，可以大幅度提高管理的便捷性。

3.4 OWASP前10大移动安全风险与MIC SMW方案

采用多信云安全移动办公解决方案（MIC SMW），能够有效解决OWASP前10大移动安全风险，具体见下表：

4.3 表3-1 OWASP前10大移动安全风险与MIC SMW方案对比

Category	2013	2014	采用 SMW 之后的风险状态
M1	Insecure Data Storage	2013 M2 + 2013 M10	app 的敏感数据不存储在员工设备上，风险可控。如果 MIC SMW 中运行的其他 app 都是高度可信的（不窥探其他 app 存储的数据，也不提供浏览 SD 卡文件系统的功能），则风险可以认为是消除。
M2	Weak Server Side Controls	2013 M1	如果攻击者无法从其他渠道获取到 app 的 apk 文件，以分析 app 和后台的业务交互行为，就无法从 app 角度寻找到对后台响应 API 接口的攻击点。
M3	Insufficient Transport Layer Protection	2013 M3	App 和后台均运行在企业内网中， 内网通信本身可以认为是安全的，出现攻击的可能性较小。
M4	Client Side Injection	2013 M8 + 2013 M10	对于从其他恶意 app 发起的注入攻击行为，MIC SMW 可以消除。但是对于使用 web view 较多的 app，仍然需要关注传统的 web 攻击方式，如 XSS。
M5	Poor Authorization and Authentication	2013 M5	企业可以利用 MIC SMW 的 SSO 功能，提高 app 的身份认证安全性和易用性。
M6	Improper Session Handling	2013 M9	MIC SMW 本身的身份验证机制，可减轻 app 在 session 过期管理方面的潜在缺陷。
M7	Security Decisions via Untrusted Input	2013 M4	MIC SMW 中配置的其他 app 是安全的（MARS 集成），不会发起恶意输入。
M8	Side Channel Data Leakage	2013 M7	App 即使存储了敏感数据，也不会泄漏到员工设备上。管理员还可以利用 MIC SMW 在 Android 平台上的反截屏功能来防止信息泄露。
M9	Broken Cryptography	2013 M6	如果 app 使用了不安全的加密算法，由于其存储的数据在企业内网中，攻击者无法轻易获取这些数据。
M10	Sensitive Information Disclosure		如果攻击者无法从其他渠道获取到 app 的 apk 文件来进行逆向分析，则风险可以认为消除。
	Lack of Binary Protections		如果攻击者无法从其他渠道获取到 app 的 apk 文件来进行逆向分析，则风险可以认为是消除。

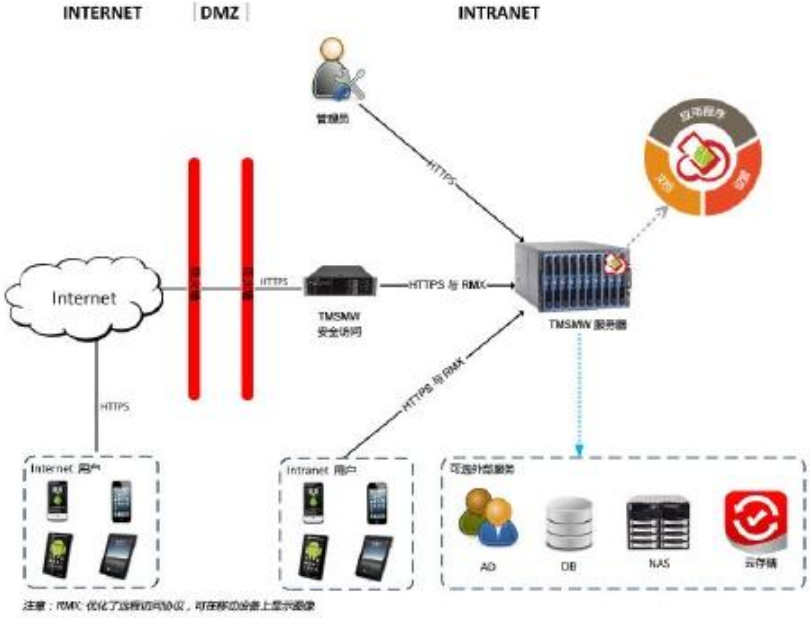
第四章 多信云安全移动办公架构（SMW）介绍

4.1 Safe Mobile Workforce架构

根据企业组织的规模和需求，多信云科技安全移动办公软件可以部署单个或多个服务器和安全访问。依托多个服务器，安全移动办公平衡服务器之间的负载能力，可以实现最高效率。

1. 单个服务器安装模式

单个服务器安装模式是指仅一个安全移动办公服务器和安全访问的部署。



2. 多个服务器安装模式

多个服务器安装模式是指多个安全移动办公服务器和安全访问的部署。

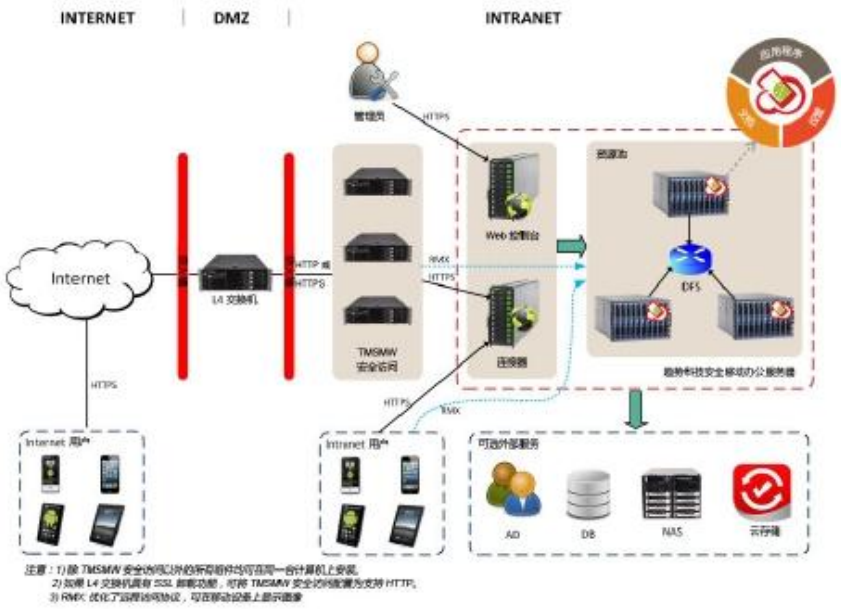


表4-1 多信云安全移动办公系统组件构成表

组件	描述	必需或可选
安全移动办公服务器	安全移动办公服务器包含 Web 控制台、Web 服务、控制器和资源池。Web 控制台为管理员提供中央管理控制台。Web 服务管理用户登录、注销以及与用户工作区的连接。控制器允许 Web 控制台管理资源池、资源池托管工作区。每个工作区都作为一个安全移动办公实例运行。	必需
安全移动办公移动客户端应用程序	多信云办公应用程序安装在移动设备上。客户端应用程序与安全移动办公服务器连接，以允许用户使用服务器上托管的工作区。	必需
安全访问服务器	安全移动办公安全访问使移动客户端可以通过 Internet 访问安全移动办公服务器。	可选
Active Directory/OpenLDAP	安全移动办公服务器从 Active Directory 或 OpenLDAP 导入组和用户。	可选
外部数据库	外部数据库为用户数据提供可扩展的数据存储。缺省情况下，安全移动办公服务器在其本地硬盘驱动器上维护数据库。但是，如果要将数据存储在外部位置，则需要配置外部数据库。	可选
外部存储	通过使用此选项，可以将用户数据存储在外部存储中。	可选
云存储服务器	云存储服务器为所有用户提供文件存储。	可选

3. 为什么使用安全访问服务器

安全移动办公安全访问，使移动设备客户端可以通过Internet安全访问移动办公服务器。如果要避免安全移动办公服务器暴露在Internet上，甚至不暴露在DMZ中，您需要安装安全访问，通过L4交换机安装多个安全访问来进行负载平衡。使用安全访问的优势如下：

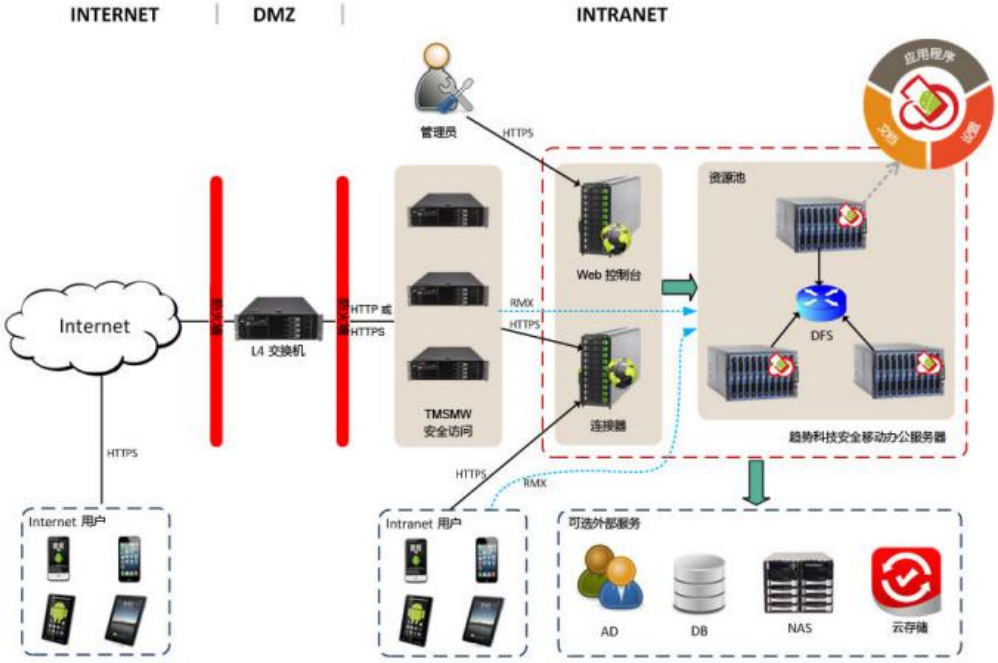
如果使用安全访问，则仅需要为移动客户端打开一个IP地址和一个端口号。安全访问通过HTTPS接收移动设备客户端注册请求，并将其中继到安全移动办公服务器，通过安全访问和安全移动办公服务器使用防火墙，进行出站网络连接，以确保安全性。

安全访问可以部署在DMZ或Intranet中，使用单个或两个网卡：如果您在不同的网络中配置Internet移动设备和安全访问，则只需一个网卡。如果在同一网络中以桥接模式配置Internet移动设备和安全访问，则需要两个网卡。在此模式下，一个网卡提供移动设备客户端和安全访问之间的连接，另一个网卡连接安全访问与安全移动办公服务器。

4. 2 Safe Mobile Workforce部署

MIC SMW安全访问：移动互联网使用者由MIC SMW安全访问网关连接MIC SMW服务器后，使用MIC SMW所提供的服务。SA可以部署于DMZ区域，以避免SMW因置于DMZ区域暴露于网络安全的风险中。

MIC SMW服务器：提供虚拟移动平台服务，用户连线之后可使用企业提供的Android APP及Web Clip取得内部资源。假设内部办公人员为2000人，并发率为10%，则估计会有200个并发。SMW硬件需求以最大同时连接数400人进行规划，需要准备两台SMW服务器，搭建HA模式。MIC SMW安全访问网关服务器需要准备两台，通过四层交换机实现负载均衡。

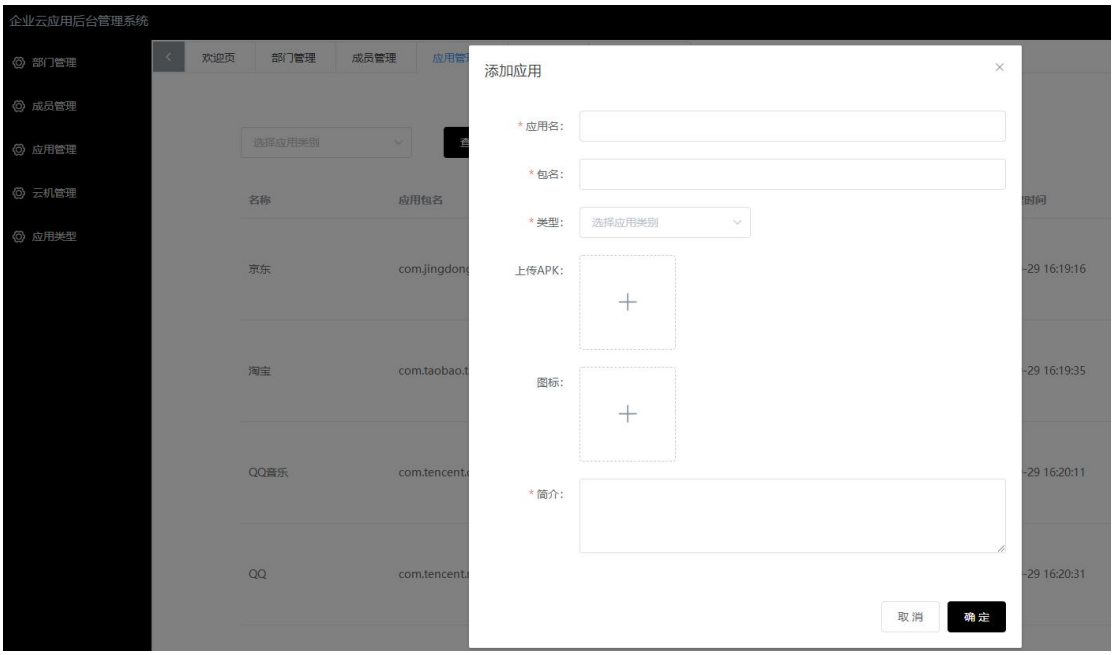


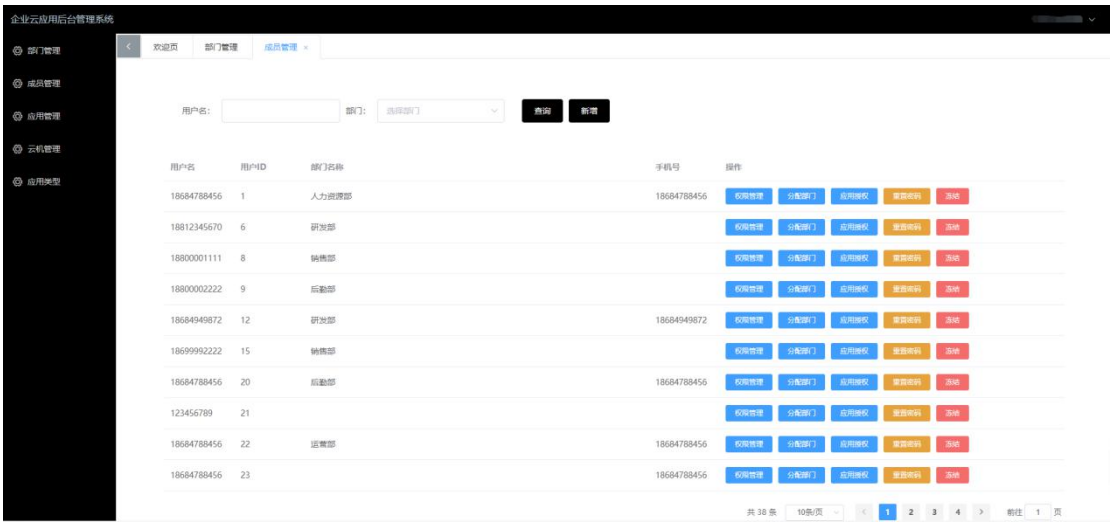
4.3 Safe Mobile Workforce功能模块

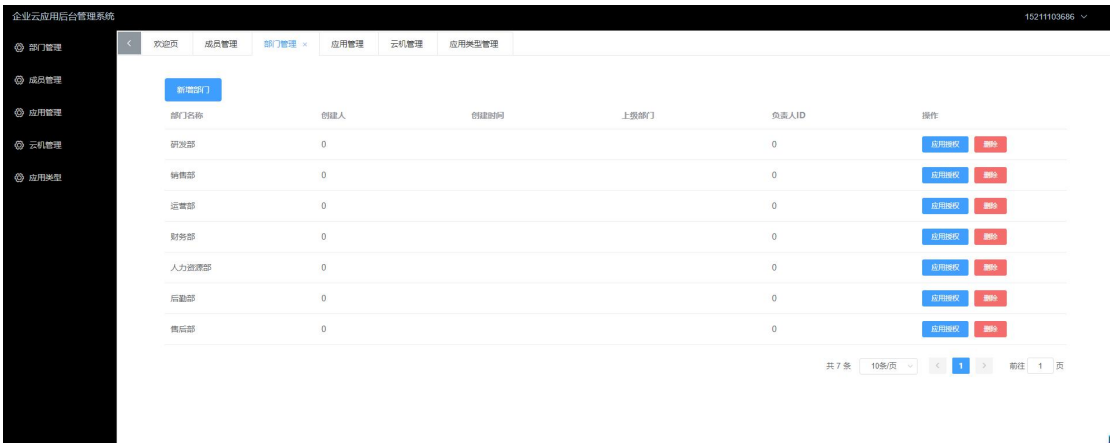
表 4-2 Safe Mobile Workforce 功能模块介绍

功能	描述
数据保护	所有企业应用程序和数据都保存在管理员控制的公司安全服务器上。
移动 APP 安全扫描	所有企业上传的 Android 应用，均经过多信云科技移动安全信誉评估服务的扫描，确保发布应用的安全性。
美好的用户移动化体验	用户可使用个人移动设备访问公司数据，因此可保留移动操作系统用户体验；系统易于使用，可访问公司虚拟工作区；智能手机和平板电脑的自然屏幕触摸体验。
简化的管理	管理员可从单个 Web 控制台集中管理所有用户。
单点登录 SSO	缩短在虚拟工作区中重新输入密码所用的时间；通过减少有关密码的 IT 服务台呼叫数，以降低管理成本。
工作区定制	管理员可为每个员工创建个人虚拟移动工作区；管理员可从服务器为员工在其虚拟工作区中集中定制应用程序。
单点登录	包括用于准备应用程序进行单点登录的应用程序-封装程序技术，而无需应用程序开发人员进行处理。

基于用户的配置文件	提供基于用户的配置文件管理；用户可从其任何移动设备使用自己的虚拟工作区。
可管理的生命周期	管理员可远程管理工作区的整个生命周期，从生命周期的置备到结束。
自带安全操作系统	为简单部署提供独立式基于 ARM CPU 的 Linux 的操作系统。
与多信云科技云存储集成	提供与多信云科技云存储的集成，从而为所有用户提供基于云的文件存储。
与企业基础架构集成	提供与 LDAP 和外部存储的集成。
显示/隐藏内置应用程序	使用户可以在用户工作区显示或隐藏电子邮件、浏览器、下载、日历、联系信息、计算器等内置应用程序。
改进的客户端性能	通过优化移动设备的内存和 Internet 带宽，显著改进了移动客户端性能，从而为用户提供更好体验。
禁用屏幕截图（针对 Android）	禁止用户在其移动设备上进行工作区的屏幕截图。
支持高可用性	增加了高可用性 (HA) 支持以确保不间断地提供服务。
增加了“画质优先”和“速度优先”选项	可以在移动设备上选择画质优先或速度优先选项，以优化 Internet 带宽并改进用户体验。
绕开代理服务器设置	新增了支持适用于工作区的绕开代理服务器设置。
OAuth 2.0 身份验证支持	为用户注册增加了 OAuth 2.0 身份验证支持。
用户状态重置设置	增加了一个选项，可以配置经过多长时间之后服务器会将用户状态从空闲重置为脱机。
电子邮件通知	在实际移动设备上增加了电子邮件通知功能，可以在用户工作区收到电子邮件时向用户发出通知。
客户端版本验证	增加了注册前验证安全移动办公客户端软件版本的功能。如果客户端软件版本与所需版本不匹配，则不会注册客户端。
轻松上传应用程序	为管理员提供单独的应用程序 (MIC SMW App Push)，方便管理员将应用程序上传至安全移动办公服务器。
重塑品牌工具	包括自定义产品品牌项目的工具，如产品名称、标志、标题、图像、服务器地址以及安全移动办公服务器和客户端应用程序中的其他品牌项目。







第五章 多信云终端开发规划

多信云终端致力于解决政企办公安全问题，帮助企业实现办公便捷化、数字化。端云一体、端云协同是5G重要的应用方向，手机应用及办公软件等在云端运行，终端通过屏幕和网络访问、操作，将带来全新的办公体验。

针对移动办公场景，多信云科技已推出多信云安全移动办公解决方案。依托虚拟化、自动化及云计算技术，多信云科技将进一步加强技术研发，深入挖掘、分析企业PC办公领域的数据安全保护需求，适时推出多信云安全办公PC端解决方案。

面向未来，为了满足多场景与不同屏幕的灵活使用，多信云科技将借助ARM架构实现PC虚拟办公系统与移动虚拟手机多屏互通生态的建立。一套云端系统，在电脑、手机、ipad等不同的端口，随着端口的切换，界面将根据设备的不同而显示不同的操作界面，同一个应用也会随着设备的更换而适应显示形式、操作逻辑，实现终端上云，多屏一体的开创性局面。

多信云科技简介

厦门多信云科技有限公司（简称多信云科技）是一家从事一体化云系统服务及提供云终端技术平台的企业，致力于在5G环境下为全行业提供云服务解决方案，助力全行业实现数字化转型与升级。

多信云科技是华为战略合作伙伴，与华为在云计算、人工智能、华为云鲲鹏云服务等方面进行全方位、深层次的战略合作，共同开展“5G+云+AI”计算层面的合作布局，为全行业提供安全、高效、便捷的云服务解决方案。

站在5G时代的风口中，多信云科技在云手机、云办公等领域重点布局。公司整合虚拟化技术、自动化技术优势及华为云AI能力，采用全球领先的虚拟技术架构，推出多信云安全移动办公解决方案，以满足政企在不同场景下的移动安全办公需求。基于多信云安全移动办公解决方案，办公“虚拟手机”集中部署在云端数据中心，数据不落地，业务开展更灵活，安全级别更高，能够有效确保政企信息安全，助力政企数字化转型升级，全面开启移动安全办公新时代。

多信云科技聚焦ARM赛道，致力于成为5G时代的硬科技企业。多信云科技团队核心成员来自于腾讯、百度、VMware、搜狐、移动、盛大、网龙、IGG等一流互联网及科技企业，在虚拟安全办公领域有深厚的技术积累及丰富的实践经验。

未来，多信云科技将与华为联合开展5G+Cloud+X场景下的业务创新，深入探研AI+云手机的垂直场景应用，全面推动多信云终端在政务及企业办公应用场景落地生根，共同缔造更美好的数字世界。

参考资料：

1、中国互联网络信息中心（CNNIC）,2020 年 9 月，第 46 次《中国互联网络发展状况统计报告》，网址：http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/202009/t20200929_71257.htm

2、中国互联网络信息中心（CNNIC）,2021 年 8 月，第 48 次《中国互联网络发展状况统计报告》，网址：http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/202109/t20210915_71543.htm

3、QuestMobile，2021 年 11 月，《2021 中国移动互联网秋季大报告》，网址：https://www.questmobile.com.cn/research/report-new/177

4、艾媒咨询，2021 年 3 月，《2020-2021 年中国 OA 行业研究报告》，网址：https://report.iimedia.cn/repo236-0/39375.html?acPlatCode=sohu&acFrom=bg39375

5、国家网信办，2020 年 7 月，《数字中国发展报告（2020）》，网址：http://www.gov.cn/xinwen/2021-07/03/content_5622668.htm

6、工信部副部长辛国斌：我国已建成 5G 基站超百万个，5G 终端超 4 亿部，2021 年 09 月，网址：https://www.163.com/dy/article/GKUDTKP2051288FS.html

7、张勇敢,章伟飞,张森洪.1～6G 移动通信系统发展综述.信息与电脑(理论版),2020,32(17):157-160

8、李炜炜,袁军.融合视角下媒介素养演进研究:从 1G 到 5G.现代传播(中国传媒大学学报),2019,41(09):161-165

9、邬贺铨，2021 年的 5G 应用更超乎想象，2021 年 1 月，网址：https://baijiahao.baidu.com/s?id=1689370352707099709&wfr=spider&for=pc

10、《阿里巴巴新基建洞察之 5G 智能经济应用场景研究报告》，2020 年 06 月，网址：https://developer.aliyun.com/article/764268

11、普华永道、中国信息通信研究院、平安金融安全研究院，《2018-2019 年度金融科技安全分析报告》，2019 年 10 月，网址：https://www.163.com/dy/article/EU3JQ2SN0511DJT9.html

12、IBM Security，《2021 年数据泄露成本报告》，2021 年 8 月，网址：http://www.199it.com/archives/1296917.html

本白皮书所引用的所有参考信息和资料（非多信云科技自有业务部分），均来源于网络公开报道。

厦门多信云科技有限公司

• 厦门 • 福州 • 长沙