基于Docker容器的信创云手机产品的研究与应用实践

Research and Application Practice of ITAI Cloud Mobile Phone Product Based on Docker Container

陈 飏,侯玉华,李兴新(中讯邮电咨询设计院有限公司,北京 100048)
Chen Si,Hou Yuhua,Li Xingxin(China Information Technology Designing & Consulting Institute Co.,Ltd.,Beijing 100048,China)

摘 要:
国家“十四五”规划明确将网络安全列为新兴数字产业,针对党政军企等行业用户对移动办公解决方案的增强级安全需求,需加强网络安全基础设施建设和网络安全关键技术研发,实现“关键领域安全可控”的目标。依托信创芯片技术、操作系统、Docker容器、云原生安全等系列核心安全技术,提出一体化安全解决方案,推出面向政企行业的5G移动信创云手机产品概念,实现端到端的移动信息安全,在5G移动和信创安全领域形成技术突破。

关键词:
信创产业;Docker容器;云原生安全;云手机;政企移动办公
doi:10.12045/j.issn.1007-3043.2025.04.006
文章编号:1007-3043(2025)04-0032-06
中图分类号:TN929.5
文献标识码:A
开放科学(资源服务)标识码(OSID):

Abstract:
"The 14th Five-Year Plan" clearly lists network security as an emerging digital industry. In response to the enhanced security needs of users in industries such as the government, military and enterprises for mobile office solutions, it is necessary to strengthen the construction of network security infrastructure and the research and development of key network security technologies, and achieve the goal of "controllable security in key areas". Based on a series of core security technologies such as ITAI(information technology application innovation industry) chip technology, operating systems, Docker containers, and cloud native security, it proposes an integrated security solution and launches a 5G mobile ITAI cloud phone product concept for the government and enterprise industries, achieving end-to-end mobile information security and forming a technological breakthrough in the fields of 5G mobile and ITAI security.

Keywords:
ITAI industry;Docker container;Cloud native security;Cloud mobile phone;Government and enterprise mobile officing

引用格式:陈飏,侯玉华,李兴新. 基于Docker容器的信创云手机产品的研究与应用实践[J]. 邮电设计技术,2025(4):32-37.

0 引言

国家“十四五”规划提出 “关键领域安全可控”,明确了“加强网络安全保障体系和能力建设”相关的系列重点工程和重大任务,要求全面提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力,为开启全面建设社会主义现代化国家新征程、向第二个百年奋斗目标奋进提供可靠的网络安全保障。“十四五”纲要提出加强原创性科技攻关、提高高端芯片、操作系统、人工智能算法等关键领域研发突破与迭代应用,并将增强信创供应链安全保障能力列为重点工作。信创产业是实现“十四五”规划发展的重要抓手,更是实现高质量发展和改革创新的核心内容[1-2]。

随着5G网络的普及,移动办公已成为固定办公不可缺少的重要补充手段,党政军企等行业用户急需安全、稳定且便捷的移动办公解决方案,云手机具备成

收稿日期:2025-02-21

本低、安全性高等特点，可满足用户需求。当前云手机市场还在起步阶段，全球范围内的用户规模相对较小，用户接受度和市场渗透率仍然保持较低水平。随着5G网络的快速发展，政企行业越发关注信息安全，国内信创产品趋于成熟，信创云手机作为云手机产品中最具优势的产品，其市场必然呈增长趋势[3-4]。针对政企等行业应用的5G移动安全增强级要求，急需研究端云一体化安全解决方案。本文提出面向政企行业的5G移动信创云手机产品概念，在5G移动和信创安全领域形成突破[5-7]。

1 信创云手机产品概述

信创云手机产品以国产飞腾CPU和麒麟操作系统为安全底座，通过在信创服务器上创建虚拟手机为行业用户提供云手机服务，用户仅需在个人手机上安装云手机客户端APP，即可随时随地通过移动终端进行移动办公，确保企事业数据和应用的终端零留存、不泄露。信创云手机产品示意如图1所示。

在云侧，基于由飞腾CPU和麒麟操作系统组成的PK信创体系安全底座，以及国产安全技术和方案厂商，研发可运营的信创云手机平台，打造并建设国内首套信创化的5G网络云手机运营环境；在网络侧，面向信创云手机业务模式，针对性地制定5G网络保障策略，提供中国联通5G网络安全和服务集成，有效保障云手机的带宽及时延等用户体验；在端侧，组织信创终端产业联盟，共同推动信创化多形态的移动终端的成熟和孵化。从3个层面共同支撑信创云手机能力，形成贯穿端、网、云的全信创的移动安全业务体系。根据国家“十四五”规划中加强网络安全基础设施建设和网络安全关键技术研发的战略指引，实现“关键领域安全可控”的战略要求，面向政企行业和其他移动安全场景，推动信创云手机产品全面进入应用实践。

2 基于Docker容器的信创云手机技术架构

基于Docker容器的信创云手机主要分为业务运行平台、系统镜像、业务管理系统、运维管理系统、推流、客户端等6个部分，具体如图2所示。

a）信创云手机业务运行平台。信创云手机业务运行平台实现了资源容器化和集群管理功能，支持基于Docker的多云手机实例的创建、管理和回收的全周期管理，具备Android镜像实例的运行环境，未来可扩展支持鸿蒙/分形等操作系统；针对管理需求，该平台可提供实例管理和资源管理功能。信创云手机业务运行平台实现了底层信创的软硬件环境的资源虚拟化，可满足云手机实例运行所要求的各种资源支持需求。

b）信创云手机系统镜像。系统镜像在业务运行平台提供的虚拟化资源上，实现了基础镜像管理、人机交互、设备定义接口、系统兼容性、系统稳定性、外设仿真接口、日志获取和系统调试等功能，支持镜像加载以及镜像运行。

c）信创云手机业务管理系统。业务管理系统包括用户管理、应用管理、策略管理、云手机管理、系统管理等，实现了个人用户账号的注册和开通、针对个人用户配置相应的资源配置策略和安全策略、个人用

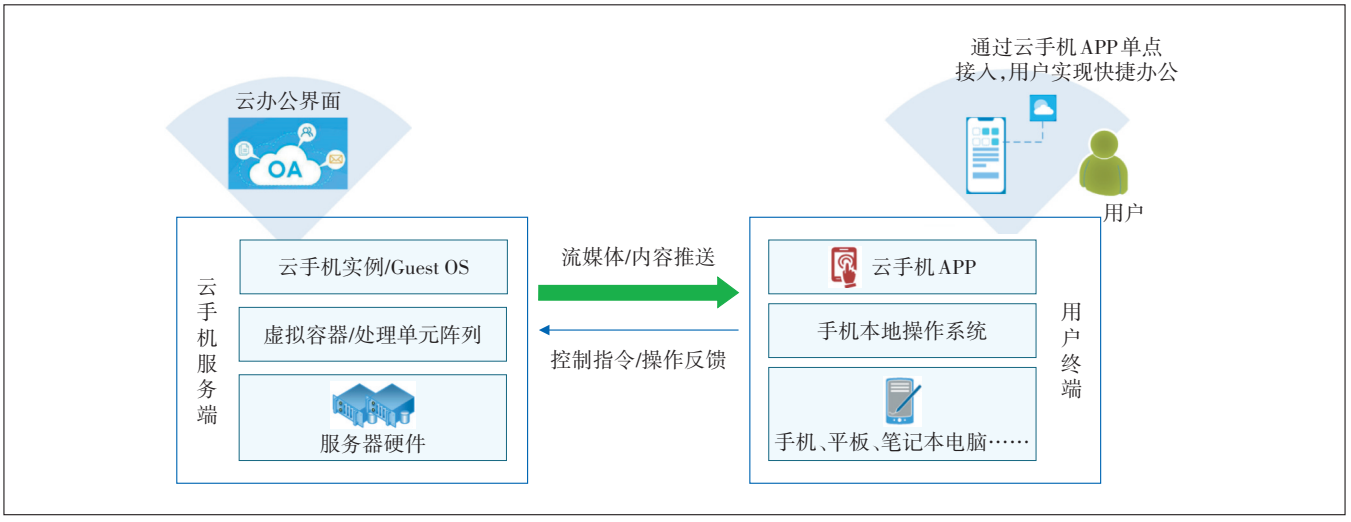

图1　信创云手机产品示意

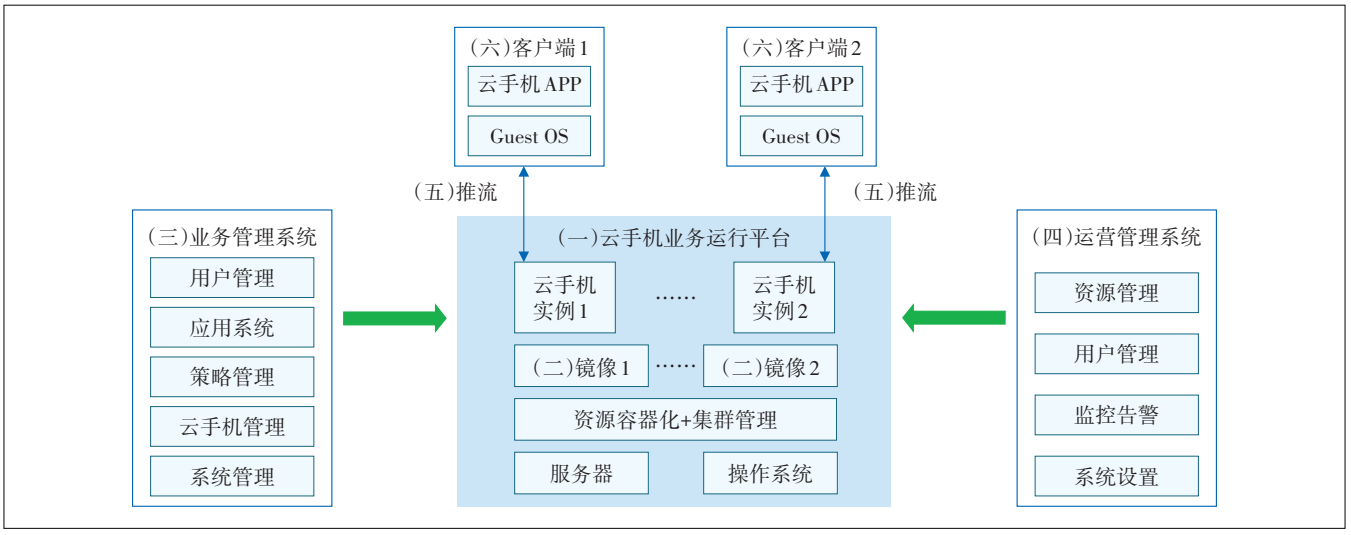

图2 信创云手机技术架构

户业务使用状态、为个人用户配置的可用的移动应用等功能。

d) 信创云手机运营管理系统。运营管理系统包括资源管理、客户管理、监控告警、系统设置等。该系统实现了系统资源的分配、监控和优化,客户信息的全流程管理,云手机系统运行状态的实时监测以及系统个性化设置等功能。

e) 信创云手机推流。云手机推流负责从平台向移动终端客户端的业务推流服务,实现了云手机实例的音视频编码和解码、音视频流传输以及客户端控制信令、客户端输入内容的回传。基于实际场景需求,信创云手机推流支持RTP、RTCP、SRTP等安全传输协议。

f) 信创云手机客户端。终端客户端完成云手机业务的登录认证和流媒体响应,同时实现终端侧设备外设虚拟化接口、终端侧控制信令生成和回传等服务。根据信创云手机业务的安全性要求,客户端同时支持对终端权限和数据管理的安全防护,对客户端用户行为提供必要的行为监控和审计。

3 信创云手机产品架构

信创云手机产品由云手机业务运行平台、业务管理系统、云手机客户端3个部分组成。信创云手机的产品架构如图3所示。

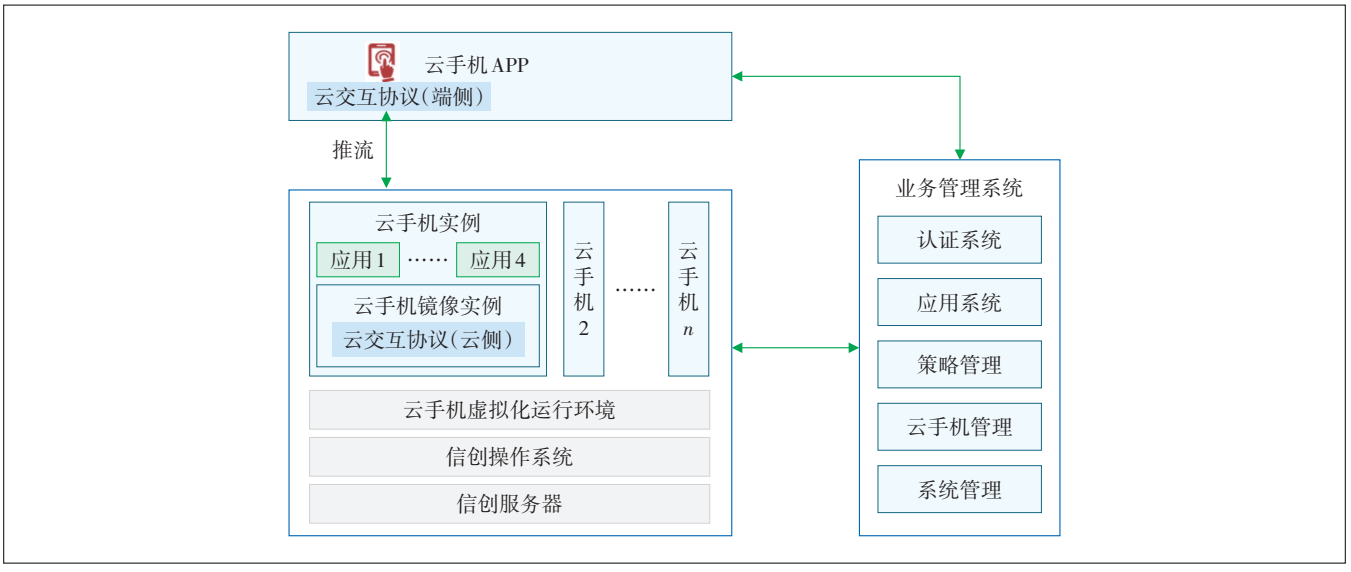

图3 产品架构

3.1 云手机业务运行平台

云手机业务运行平台是云手机的核心，它支持运行多个云手机镜像、实例和应用，同时支持云手机推流。该平台主要负责云手机核心业务的计算服务，具体包括虚拟手机操作系统、虚拟服务器系统等。

3.2 业务管理系统

业务管理系统实现对云手机的用户群、云手机实例、安全应用、安全策略、安全认证等的管理控制，包括首页概览、云手机管理、安全应用管理、安全策略管理、管理员管理、安全认证等能力。

3.3 云手机安全客户端

云手机安全客户端包括支持虚机手机画面显示、远程触控操作、实体手机外设模拟、安全防护与行为监控、企业应用商店、消息通知等能力。

4 关键技术

4.1 基于Docker容器的服务器虚拟化

Docker是一种轻量级的虚拟化技术，被广泛应用于云计算[8]、DevOps[9]等领域。Docker以容器的形式实现虚拟化，相比于传统的虚拟机技术，Docker具有更高的性能和更轻量级的特点。Docker使用Linux内核的NameSpace和Cgroup机制进行容器的隔离和资源控制，能够有效控制容器的权限和安全性[10]。

信创云手机产品采用Docker的方案，以在同一个Linux操作系统之上虚拟出多个同样的操作系统，每个应用程序运行在一个独立的Android操作系统中。基于Docker容器的服务器虚拟化架构如图4所示。

a）硬件层。信创服务器主要由飞腾芯片、麒麟操作系统和国产GPU组成，为云手机服务提供自主可控的安全底座。

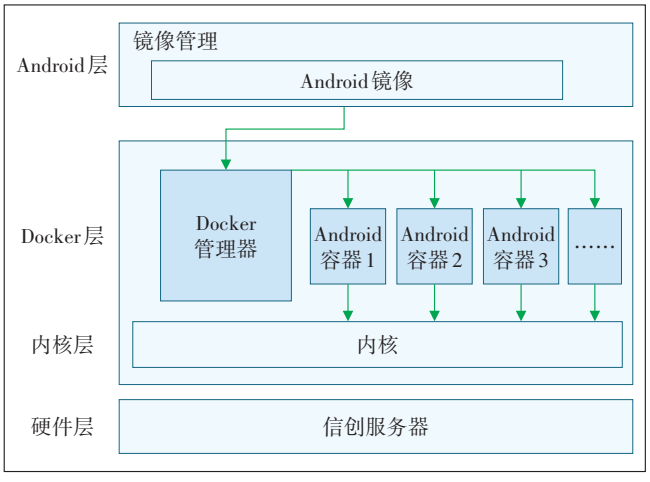

图4　基于Docker容器的服务器虚拟化架构

b）内核层。服务器虚拟化应确保内核支持Cgroup、NameSpace、binderfs、ashmem/memfd、IPv6、ION/DMA-BUF Heaps、4KB page size等功能。

c）Docker层。该层提供Docker环境和管理工具，将Docker移植到信创操作系统上，解决其与系统冲突的问题，实现Docker的正常运行。

d）Android层。云手机的Android运行环境与实体手机的Android运行环境存在一些差异，需与Docker融合，生成Docker的Android云手机镜像，使Android系统能够作为资源在Docker中加载运行。

4.2 云手机推流

云手机推流的核心是定义一套交互协议，其关键部分由服务端和客户端构成。服务端运行在云手机系统上，客户端运行在移动终端上。客户端和服务端通过基础网络连接，比如4G、5G、Wi-Fi等，实现高效的流媒体传输和控制指令传输，可以实现用户的远程操控和交互。云手机推流架构如图5所示。

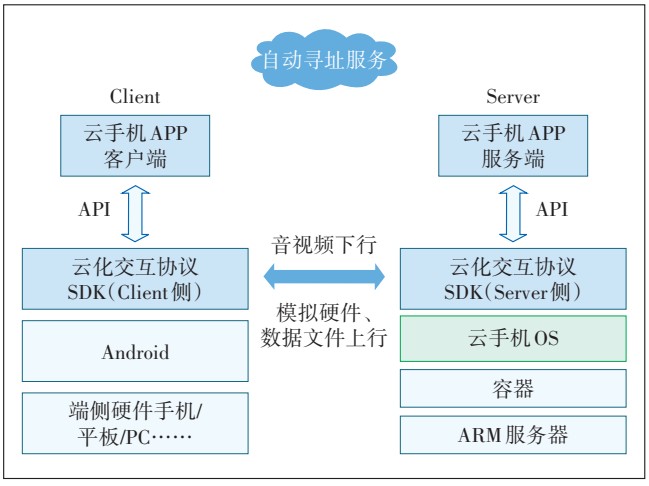

图5　云手机推流架构

云化交互协议（Client侧和Server侧）是云手机推流核心的实现层，Client侧和Server侧的交互实现了音视频从云手机下行到终端，同时在终端上采集各种模拟硬件控制流数据、文件数据等上传到云手机上。

基于云化交互协议，客户端APP需要实现用户交互界面，服务端则实现无界面的后台应用，最终完成端对端的远程交互。同时，云化交互协议提供自动寻找服务，可协助客户端实时找到可用的设备。客户端和服务端通过各种网络环境，实现即时的互联互通。

因此，云手机客户端实际包含服务端和客户端2

个部分,服务端主要功能包括账号登录、屏幕和音频数据抓取、基于云手机推流协议进行推流、接收云手机客户端发来的各种模拟输入事件等;客户端主要功能包括用户登录、连接管理、播放来自云手机推流协议的音视频帧、采集本地的触屏、麦克风、摄像头指令和数据等。

5 建设部署

信创云手机系统根据用户及并发数量,可支持单机部署和集群部署,包含云手机服务器、管理服务器、存储设备、防火墙、路由器等。信创云手机系统的建设部署架构如图6所示。

根据组织的规模和需求,云手机系统可以部署在单个或多个信创服务器上,集群部署时支持负载均衡,从而保障更高效率和使用体验,也支持弹性扩展。

信创云手机系统也支持公有化部署和私有化部署,可以与企业的业务服务器统一部署,也可独立部署。对于公有化部署,中国联通发挥运营商的网络优势,可以为客户提供安全的网络环境和信创服务器、国产GPU等基础设施,基于安全可信的基础环境为客户提供弹性可扩展的企业移动办公解决方案。

6 产品优势

6.1 信创安全底座

以国产CPU芯片和操作系统为云手机平台的基础,构建信创云手机的安全底座,底座能力安全可靠。

伴随国产信创企业不断加大研发投入,持续提升国产芯片和操作系统的自主创新能力,产业规模不断壮大,可满足不同行业和领域的需求。

通过信创产业链的资源整合,实现上下游企业的协同发展,稳步提升信创产品的性能和稳定性。

6.2 数据、应用和使用的全生命周期安全

数据的全部存储和流转在云中心,在终端没有任何存储。

a) 避免了终端系统一旦出现漏洞和病毒木马,就可能被窃取数据乃至以终端为跳板反向侵入企业网络的风险。

b) 避免了终端上移动应用存在漏洞时,应用数据较容易被分析和逆向的风险。

c) 避免了终端第三方应用通过应用间访问接口恶意窃取数据的风险。

d) 避免了终端丢失后不能及时发现和处理带来的数据外泄风险。

e) 通过明暗码水印,提升震慑力和被第三方录屏后的可追溯性。

应用全存储在云中心。

a) 统一应用出入口,更容易进行安全管控和审计,大大降低了数据出企业网的风险。

b) 可在云端拦截第三方输入法的数据上传,避免输入法采集数据的风险。

运行全部在云中心。

a) 支持统一部署和配置安全措施,达到统一等保安全,增强整体安全。

b) 所有敏感行为可追溯、可审计。

c) 用户之间强隔离,实现了虚拟机级强隔离,更安全、更可靠。

网络传输安全。

a) 显示内容以加密流媒体的方式到达用户终端,视频流进行切片并采用私有协议进行混合数据加密和压缩,并对数据包进行签名验证,以保证数据安全。

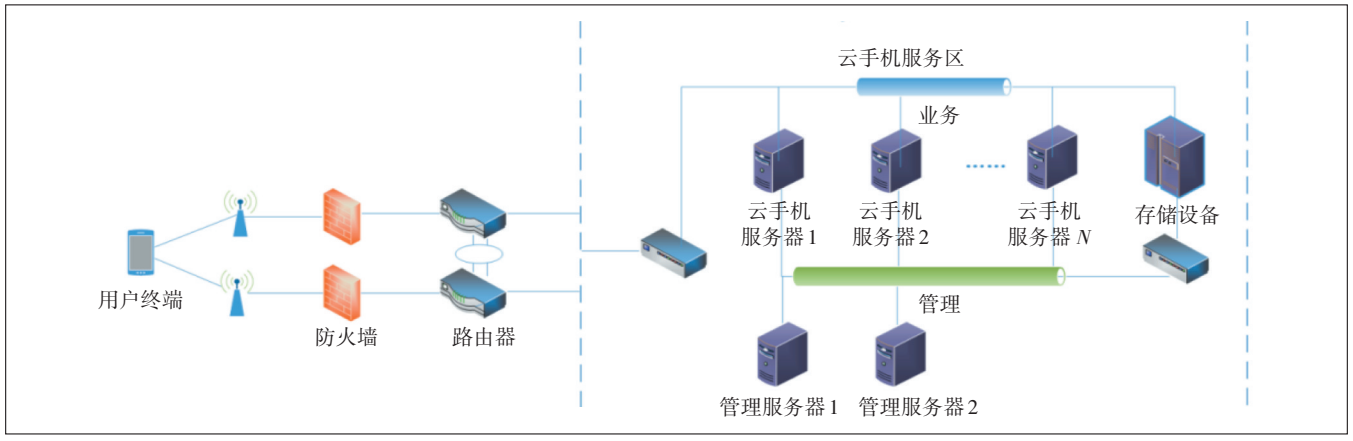

图6 建设部署架构

b）通过融合运营商网络定制能力，有效保障了网络链路安全能力和网络链路质量，打造客户端到平台端“端到端”的通信级链路安全保障。

6.3 统一管理

统一管理具有如下优势。

a）统一管理。企业IT部门能够根据前端用户的不同级别和权限，快速配置和开通应用和数据访问权限。

b）集中管控。支持随时关停风险用户访问，还可选择性地生成用户活动的审计跟踪及大数据分析等。

c）集中部署。支持与企业数据中心一体化安全防护和管控，且应用数据不出企业数据中心。

d）高效运维。支持统一或按需进行应用分发和升级，且即刻生效。

e）灵活配置。支持按照企业内部的不同岗位、不同角色定制专属的云手机。

f）简化运维。不需维护和管理多终端的设备型号和操作系统，降低了运维的复杂性。

6.4 整体成本降低

通过产业合作，提供包括Android、鸿蒙、YunOS以及其他OS的系统定制能力，可满足各种移动办公场景的需求。

企业可摆脱对繁杂移动设备的依赖，无需定制和采购用户终端。

无需考虑移动设备较容易损坏和丢失、折旧等后期成本。

降低IT人员对复杂的设备管控等的运营成本，节省人力。

单台服务器可支持几十个并发用户，按照用户并发率为10%或20%计算，单台服务器可支撑几百个用户使用，持续使用后费用远低于移动设备的采购与折旧。

6.5 企业效率和用户体验提升

对用户来说，公私分明，企业对用户手机零管控，不侵犯用户任何个人隐私。用户可随时随地随设备办公，不必担心设备丢失、更换设备等带来的应用和数据的找回迁移。

对IT管理员来说，关停处置问题用户、开通新用户、应用部署和升级等均可即开即用；整体部署或迁移极为简便。

对开发者来说，一次性开发和测试，不再考虑兼容性问题。

对企业来说，避免第二用机的低有效和低到达性，提升了沟通效率和管控效率，所有数据与操作在云端，方便数据分析。

7 结束语

信创云手机作为云计算与智能终端技术深度融合的产物，近年来在信息化领域引发了广泛关注。通过深入研究信创云手机的原理、技术实现及其在各行各业的应用，可以清晰地看到其巨大的发展潜力与广阔的市场前景。在未来，可以预见信创云手机将在信息化建设和政企移动办公领域中发挥越来越重要的作用，笔者将持续跟进相关技术进展，不断迭代升级信创领域云手机产品，为信创产业的数字化转型贡献更多的智慧和力量。

参考文献：

[1] 易辰. 信创产业迎来高质量发展新契机：数智化技术驱动新一轮创新[EB/OL]. [2024-08-21]. https://www.ecinc.com.cn/article/2022/a2429399948f4f13a0fa3a36bcd08d3e.html.

[2] 吕伟. 芯片行业专题报告：信创从“芯”开始[EB/OL]. [2024-06-13]. https://news.qq.com/rain/a/20220613A01LR100.

[3] 王莉，王智，王丽珍. 基于云计算的数据安全存储策略探析[J]. 网络安全技术与应用，2021(6)：68-70.

[4] 赵俊，瞿伟峰. 探讨信创系统网络安全问题及策略[J]. 网络安全技术与应用，2022(4)：11-12.

[5] 周栋. 信创混合云管理平台的设计与实现[J]. 信息系统工程，2022(3)：52-55.

[6] 莫洋，王耀南，刘杰，等. 我国智能机器人核心芯片技术发展战略研究[J]. 中国工程科学，2022，24(4)：62-73.

[7] 刘仲驰. 基于国密算法的通信数据加密传输方法[J]. 数字通信世界，2023(3)：24-26.

[8] 苗春雨，杜廷龙，孙伟峰，等. 云计算安全关键技术、原理及应用[M]. 北京：机械工业出版社，2022.

[9] 哪吒. DevOps是什么？DevOps能够给我们带来什么？[EB/OL]. [2024-02-26]. https://blog.csdn.net/guorui_java/article/details/129213073.

[10] 刘文懋，江国龙，浦明，等. 云原生安全攻防实践与体系构建[M]. 北京：机械工业出版社，2022.

作者简介：
陈飓，毕业于北京理工大学，高级工程师，硕士，主要从事移动终端信息安全、云手机安全业务相关的研究工作；侯玉华，毕业于沈阳工业大学，高级工程师，硕士，主要研究方向为移动信息安全、终端操作系统等；李兴新，毕业于北京航空航天大学，高级工程师，硕士，主要从事移动终端信息安全相关的研究工作。