2014

密级：公开

产品白皮书

360 天机移动终端安全管理系统

2014 年 12 月

版权声明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京奇虎科技有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京奇虎科技有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

信箱：北京市朝阳区酒仙桥路 6 号院 2 号楼　邮编：100015

电话：010-52447412

邮件：tianji-kefu@360.cn

公司简介

360 是中国领先的互联网和手机安全产品及服务供应商。据第三方统计，按用户数量计算，360 是中国第二大互联网公司，最大的互联网安全公司。

作为互联网“免费安全”的首创者，360 成立以来，秉承“用户利益至上”的原则，以颠覆式创新的模式，通过产品技术创新、用户体验创新和商业模式创新，改变了市场格局，并建构出全球互联网前所未有的“360 模式”。

创新和开放是 360 的 DNA。360 通过提供完善的平台和网络安全服务，以开放平台模式实现商业价值，与合作伙伴共同建立起多方共赢的互联网生态体系。

作为中国最大互联网安全公司，360 拥有国内规模最大的高水平安全技术团队，旗下 360 安全卫士、360 杀毒、360 安全浏览器、360 安全桌面、360 手机卫士、360 手机助手、360 搜索等系列产品深受用户好评，使 360 成为无可争议的网络安全第一品牌。

2011 年 3 月 30 日，360 在美国纽约证券交易所上市（股票代码 NYSE:QIHU ），目前，360 总市值超 100 亿美元，是发展最快的中国互联网公司。

截止 2013 年底，360 的 PC 端产品和服务的月活跃数达到 4.75 亿，360 产品的用户渗透率达到 94.6%；使用 360 手机卫士的智能手机用户总数已达 4.67 亿，市场渗透率近 70%；360 浏览器的月度活跃用户达到 3.54 亿，用户渗透率 70.4%，在国产浏览器中处于领先地位；360 个性化起始页和其子页面的日均独立访问用户为 1.19 亿人，日均点击量约为 6.81 亿次；360 手机助手用户数超 3 亿，累计下载次数达 320 亿以上，是中国最大手机软件游戏下载平台。目前，360 搜索市场份额达到 24%，成为中国搜索市场的重要参与者。

目录

一 前言

随着智能终端的成熟与普及，以手机、平板电脑为代表的个人智能终端设备逐渐进入企业领域。众多企业已经开始支持员工在个人移动设备上使用企业应用程序，员工使用个人智能终端设备办公已经成为一种无法逆转的潮流。这类被称为 BYOD(Bring Your Own Device，自带设备办公)的现象为企业带来了全新的机遇：

- 降低成本和投入

允许员工自带设备办公，消除了硬件采购和维护费用，为企业节约了大量的 IT 成本。

- 拓展企业业务

为企事业单位提供了更为丰富的办公和业务拓展渠道。例如，交警通过移动终端实时处理交通事故数据，金融企业利用平板电脑为客户展示产品方案、办理业务，制造行业通过移动终端实时获取生产流程中的各项指标等。

- 提高员工效率和满意度

员工对工作灵活性、设备个性化的需求促使员工不再将私人设备和工作设备完全区分。在很多员工看来，移动化时代的工作已不仅仅是上班时间的事情，随时随地都可以方便的接入企业系统，已经成为员工的工作习惯。企业顺势而为，为员工的移动办公设置方便、安全的环境，无疑将赢得员工的信任和支持。

BYOD 允许员工随时处于办公状态，而且当员工使用自己喜欢的设备工作时，操作将更顺手，获得更高的工作效率。

二 移动信息化带来安全新挑战

BYOD (Bring Your Own Device，自带设备办公)等移动信息化趋势为政府和企业带来了机遇，同时也为企业信息安全和管理带来了新的挑战：

◆ 打破了传统企业网络边界

企业员工的移动设备可以在任何时间、任何地点接入运营商 3G/4G 网络或公共/家庭 Wi-Fi 网络，移动信息化打破了原有的企业网络边界，正是这种边界的模糊性使移动终端成为企业信息安全体系的薄弱环节，移动终端中的企业数据也会因此暴露在来自互联网的攻击之下，因此亟需新的方法保护企业数据安全。

◆ 移动设备具有易失性，从而具有泄露企业数据的隐患

移动设备由于其便携性极易丢失，每年有 7000 万部手机丢失，其中 60%的手机包含敏感信息，而移动设备中所保存的企业敏感数据也因此面临泄密风险。Varonis 在 2013 年发布的关于企业中 BYOD 的趋势调查报告显示，50%的受访企业表示曾经丢失过储存企业重要数据的设备，其中 23%的企业遭遇了数据安全事故。设备丢失不但意味着敏感商业信息的泄漏，所丢失的设备也可能会变成黑客攻击企业网络的跳板。

◆ 员工主动泄密，给企业带来数据泄露的损失

根据调查，尽管 85%的企业采取了保密措施，但仍有 23% 的企业发生过泄密事件，员工的主要泄密途径除了拍照泄漏、存储在手机中进而外泄外，还有离职员工拷贝企业重要信息，从而出卖资料。员工的这些行为，导致企业重要信息无意或有意泄密，不仅为企业带来财产损失，影响企业的业务运营，还带来了商誉受损等问题。

◆ 移动操作系统的碎片化问题严重，统一管理不便

据 360 的统计数据，截止到 2013 年底，仅 Android 设备就有 2 万多款不同型号，员工自带的设备多种多样，如何保证策略执行的一致性、如何在一个统一的平台上管理各种设备是企业面临的另一个挑战。

◆ 应用质量参差不齐，应用市场安全性堪忧

根据 360 的数据统计，仅 2012 年全年以及 2013 年 1 月、2 月，伪造、篡改的应用就感染了近 2 亿人，78%的知名应用被盗版，如何保证员工使用的应用没有安全问题，如何保证企业的内部应用不被伪造、篡改、植入代码为企业带来了挑战。同时，根据 360 的数据分析，第三方应用市场及论坛仍然是恶意程序传播的主要途径（占 61%），最不安全的某小型应用市场的恶意程序占比竟高达 20.2%，应用市场的安全性堪忧。

◆ 手机病毒数量和类型的高速增长，使移动设备成为渗透企业网络的跳板

在移动互联网越来越深入人心的今天，攻击者们已经开始将视线由 PC 转向了移动设备。同时，由于 Root 权限滥用和新的黑客攻击技术，移动设备成为滋生安全风险的新温床，容易成为黑客入侵渗透企业内网的跳板。2014 全年，360 互联网安全中心累计截获 Andriod 平台新增恶意程序样本 326.0 万个，较 2012 年、2013 年分别增长了 25.3 倍与 3.86 倍,平均每天截获新增恶意程序样本近 8932 个；累计监测到 Andriod 用户感染恶意程序 3.19 亿人次，较 2012 年、2013 年分别增长了 5.17 倍和 2.27 倍。平均每天恶意程序感染量达到了 87.5 万人次。

◆ 公私数据混用，个人隐私难以得到保障

同一移动终端设备上既有个人应用，又有企业数据和应用，个人应用可以随意访问、存取企业数据，企业应用同样也会触及到个人数据。如何明确区分并隔离移动终端上的企业/私人数据与应用，禁止企业数据被个人应用非法上传、共享和外泄，同时禁止企业应用访问个人数据，尊重移动终端上的私人数据是一个难以避免的问题。

三 360 天机移动终端安全管理系统

360 天机移动终端安全管理系统（以下简称“360 天机”）是奇虎 360 公司基于移动终端安全所发布的一套面向企业的移动安全解决方案，能够有效地监测和管理移动终端的使用情况，保障终端数据的安全，提高自带设备用户的使用体验和工作效率。

该产品充分的利用了 360 多年来在安全领域的技术积累，以及多年来在互联网产品中摸索的成果，充分的结合了 360 手机卫士，360 云盘，360 手机桌面，360 文件管理器，360 通讯录和 360 手机助手等产品亮点，加上最新研发的国内领先的公私隔离与安全技术以及国际领先的应用集成等技术，形成了一套全面且强大的移动终端安全管理系统。

3.1 产品定位

360 天机移动终端安全管理系统致力于解决企业在向移动办公拓展过程中面临的安全、管理以及部署等各种挑战，帮助企业在享受移动办公带来成本下降、效率提升的同时加强对移动设备的管理控制以及安全防范。

360 天机解决了企业移动办公过程中的安全问题，使得企业更安全地推行移动信息化，企业不用再担心移动终端受到木马病毒的威胁从而泄露企业数据的问题、移动终端丢失或者被窃而导致的企业数据泄露问题、移动终端成为入侵企业网络的渠道问题、以及员工恶意泄密问题。

360 天机解决了企业移动办公过程中的管理问题，企业管理员可以更加高效的管控移动终端，可制定灵活可控的安全策略，提升移动终端的安全指数，可通过多样化的图表以及日志记录，更直观的查看全局状态以及追踪可能的问题细节。

360 天机使得企业员工在享受 BYOD 给自己的工作带来的灵活性和个性化的同时，解决了员工个人隐私的安全性以及工作和个人生活的平衡性问题。天机采用工作区数据和个人区数据完全隔离的方式，个人区不能访问工作区数据，同时工作区也不能访问个人区的数据

和应用，保证了个人数据的隐私和企业数据的安全，真正的实现了“一机两用”。在非工作时间员工可仅使用个人区，也很好的保证了个人生活和工作的平衡。

3.2 产品架构

360 天机移动终端安全管理系统由两部分组成：

- 基于 web 的管理中心
- 移动客户端

☑ 企业管理中心

360 天机管理中心是基于 web 的管理系统，管理者通过管理中心可以查看管辖范围内的移动终端使用情况，实施各项操作。

管理中心部署在企业内网服务器，为便于中小规模企业使用，奇虎 360 提供公网服务器管理中心服务。对于部署在内网服务器的管理中心，首次部署时将指定一个管理员账号，登录成功后可以在管理中心指定其他管理员。对于使用公网服务器的管理中心，管理员需要向天机工作人员提交申请，经认证通过后开通其所提交账号为管理员账号。

管理中心可以通过浏览器直接访问，为确保管理中心正常运行，您的浏览器需要满足以下条件：

浏览器内核为 IE6.0 或更高版本，或者 Chrome 内核

☑ 客户端

360 天机客户端部署在企业需要管理的移动终端上，企业可通过客户端实施管理中心下发的安全策略，员工可通过客户端安全地访问企业内网和办公。

为确保客户端正常运行，您的移动终端系统需要满足以下条件：

Android 4.0 及更高版本，或 iOS 7 及更高版本

3.3 产品功能

360 天机移动终端安全管理系统包括安全管理平台和移动客户端两个部分，通过管理平台对装有移动客户端的终端进行安全管理，提供对终端外设管理、配置推送、系统参数调整等，同时结合管理员可控的安全策略机制，实现更全面的安全管控特性，有效的解决了企业在移动办公过程中遇到的数据安全以及设备管理的问题。

3.3.1 安全管理平台主要功能：

安全管理平台主要包括设备管理，应用管理，内容管理三大功能，所有移动设备、移动应用、移动内容的情况都可在管理平台上进行可视化展现，并可灵活自定义首页展现的内容和方式，使企业更方便的对终端设备和应用进行快速查看和管理。

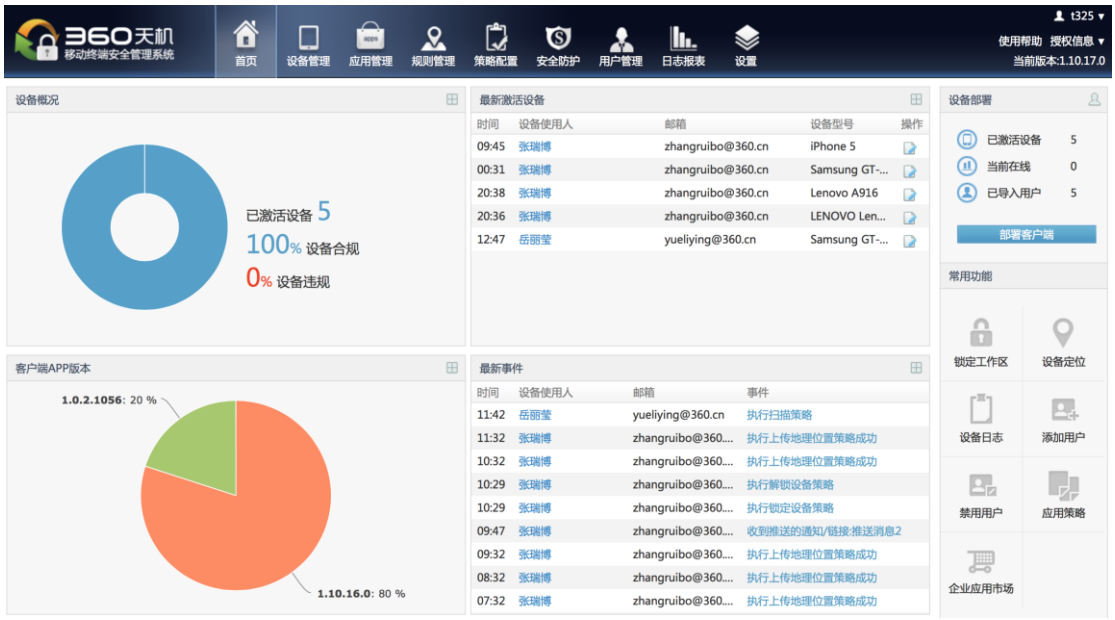

图 1 管理中心首页

☑ 设备管理（MDM）

为了更好的对移动终端的安全进行管理，天机提供了各种集中管理控制的功能，使得管理员对终端设备从注册，使用，到删除的整个设备全生命周期都能完全掌控。查看每个设备的所有权和是否活跃、是否锁定工作区、是否锁定设备、是否注销、是否激活等状态。

360 天机的设备管理（MDM）提供强大的设备指令下发、地理定位管理以及安全策略管理的功能。

管理员能通过管理中心看到每个移动终端的详细信息，并可对指定或者所有的终端进行清除工作数据、恢复出厂设置、下发锁屏密码、锁定设备、锁定工作区、启动关闭鸣响、推送消息链接等强制指令的下发

360 天机提供了用户及分组管理功能，通过分组，可将员工更结构化的管理，方便查找和管理。新注册的设备可规划到相应的分组，管理员还可根据不同分组下发相应的安全策略，满足了不同分组用户的需求。离职员工可以一键处理，清除企业数据并且不能再用离职员工的账号登录系统。

管理员可自定义移动终端的安全策略，在强管控和灵活管控之间自由平衡，可根据需要设置离线设备的处理方式、工作区密码复杂度、在指定时间或指定地点范围禁用摄像头、禁用 WIFI、禁用移动数据网络、禁用蓝牙的功能等，禁止企业的员工泄露企业数据。可根据组织架构、分组下发安全策略。

地理位置维度允许管理员查看移动终端的当前地理定位以及一周内的移动轨迹，方便对员工的行踪进行管理。

360 天机可对移动终端设备进行多项安全违规检测，包括设备是否 root/越狱，离线是否超过指定时间，是否未安装安全软件，是否已卸载天机客户端，当月流量是否超过限定值等。对于违规设备，管理员可进行清除工作数据、锁定设备、锁定工作区等强制性操作。

为了审计管理员以及企业员工所进行的操作，天机提供了日志报表功能，控制端可以记录并展示管理员的操作、时间和结果，设备的违规事件，执行策略、拦截事件和日常事件等。

图 2 设备管理

☑ 应用管理（MAM）

天机企业管理中心建立了一个专用的工作区空间，用于生成企业私有的应用市场，该市场不仅很好的规范了企业移动设备应用的下载和使用，保证了应用的安全性，而且提高了管理员统一管理企业移动应用的效率。

为了保证企业移动应用的安全性，天机采用了应用加固技术，对上传到企业应用市场的应用进行封装加固处理，可以有效预防企业应用遭受逆向威胁，保证工作区内使用的移动应用安全可靠。

管理员对终端应用有绝对的管理权限，支持对安卓和 ios 两种操作系统的应用下发，并可实施安全策略管理，可强制安装、强制卸载终端应用，可并可设置应用黑白名单，黑名单中的应用不能安装，白名单中的应用必须安装并且不能卸载。并可以查看安装统计数据情况。

管理员可自定义客户端工作区办公套件，并可对下发的应用进行升级更新管理。

图 3 应用管理

☑ 内容管理（MCM）

天机在移动终端建立了一个安全独立的工作区，采用的公私隔离技术很好的将企业数据和个人数据完全隔离，所有的企业应用和数据存储在受保护的安全工作区内，避免非法存取企业数据，使 IT 部门能更好地保护企业的应用和数据，也为员工提供了无差别的个人应用体验，达到“一机两用” 的效果。

360 天机采用 AES256 算法以及 SM 系列国密算法处理数据，对移动终端上的工作区内的企业数据进行高强度加密，同时提供安全可靠的密钥管理，确保企业数据在多终端复杂环境下的安全。

企业内部应用或第三方应用产生的数据，都安全的加密存储在工作区，仅工作区内的应用程序可以访问查看，保证企业数据安全地存储在工作区。

对于重要秘密文件，天机还提供阅后即焚功能，对于下方的消息或文件不会保存在本地，员工浏览完，消息和文件就会消失，让文件主人有效掌握文件控制权，从源头上保证文件资料不被泄露。

3.3.2 移动客户端主要功能

天机移动安全客户端通过工作区隔离、企业办公套件、企业数据加密、企业应用加固等功能，保证移动终端的数据和应用的安全。

☑ 工作区隔离

移动终端采用移动沙盒技术设计双区域模式：工作区模式和个人区模式。工作区数据应用和个人区数据应用完全隔离。提供员工办公效率同时提高设备使用率。

☑ 数据存储和通讯加密

工作区内的数据无论是存储还是通讯都经过加密处理，并且企业管理员具有对设备数据的删除权限，很好的保护企业数据不被泄漏。

☑ 企业办公套件

客户端内置了企业办公的基础套件，提高员工办公效率，同时保证数据安全性。办公套件包括企业安全浏览器、企业邮件、企业私有应用市场、企业日历等。

图 4 天机工作区

- 企业安全浏览器：下载文件安全扫描、恶意网址拦截提醒、上网环境监测。
- 企业邮件：批量配置公司邮件。
- 文件管理器：可将工作中的图片文件进行统一管理和存储。
- 企业日历：企业日历和公司邮件日历同步。设定时间内将收到日历提醒。
- 企业应用市场：统一下载和更新企业应用。
- 企业联系人：独立的联系人存储（Android4.4 以下版本）
- 天机杀毒：员工可自行进行杀毒操作，随时查杀手机病毒，企业管理员也可以通过后台对员工设备进行集中杀毒策略，保证企业数据的安全性。
- 模块自定义选择：以上功能均可通过管理中心自定义开启或关闭

☑ 私有应用市场

私有应用市场提供企业管理员定义的应用的下载、安装和企业应用的升级等功能。如下图所示：

图 5 企业应用市场

☑ 消息提醒

管理员可通过综合管理平台推送信息到各个终端，可选择简单推送或者强制推送，强制推送的消息将直接弹出信息在移动终端桌面上显示。并可设置消息为阅后即焚状态，保证企业信息不会泄漏。

3.4 产品特点

360 天机移动终端安全管理系统是基于奇虎 360 多年的安全积累基础之上，采用国内领先的公私隔离与安全技术以及国际领先的应用集成等技术，为用户提供设备管理、应用管理等专业的移动设备安全管理系统，下面就对本系统的产品特色进行详细介绍。

3.4.1 国际领先的公私隔离技术

360 是国内第一大互联网安全公司，在核心安全技术上已经有了多年的积累。在多年的安全技术积累基础之上， 360 针对天机还自主研发了国内领先的公私隔离与安全技术，在移动终端上建立独立工作区，将工作数据与个人数据完全隔离，禁止任何个人应用读取、访问工作区。

3.4.2 固若金汤的数据防泄漏技术

360 天机采用了数据加密技术，对存储和运行于客户端的数据采用高强度 AES256 算法和 SM 系列国密算法处理。同时，管理中心提供远程擦除工作数据的功能，针对强管控适配设备还可以禁止内部员工在指定时间、指定地点范围使用摄像头、截屏、USB 等功能，严防数据泄漏事故发生。

3.4.3 独有的企业应用加固、集成技术

360 天机采用应用检测以及加固技术，对管理员上传到企业应用市场中的应用进行加固和封装保护，有效预防企业应用遭受病毒侵扰，预防企业应用遭受逆向威胁。同时，应用封装服务可为企业应用提供多种隔离沙箱特性，确保企业数据安全可控。

360 天机提供安全的企业应用市场，上传、下发、升级、编辑企业应用流畅灵活，同时提供应用安装统计、应用黑白名单、静默安装卸载等功能，满足企业不同维度的需求。

3.4.4 专业的防病毒引擎

360 天机集成了 360 专业的防病毒引擎，经过多年的积累维护，360 拥有国内最全的恶意样本库，查杀无死角，新病毒秒级查杀修复。保障设备免受病毒侵扰，避免移动终端被攻击者利用成为渗透企业内网的跳板。

3.4.5 统一管理平台

无论是 Android，还是 iOS；无论是三星、小米、中兴、华为，还是 OPPO、SONY、夏新，360 天机都提供统一的管理平台，供企业的管理员灵活地管理移动设备。保证管理高效、灵活可控。

3.4.6 流程优秀的用户体验

对终端用户而言，360 天机工作区界面与系统原生界面相似，用户只需要安装一个应用，即可使用其主要的办公功能，包括邮件、日历、联系人、浏览器等；而且，工作区界面和个人区界面可以一键平滑切换，便于用户理解和使用。相比于将多个功能拆分为几个独立 app 的方式，360 天机的展现方式有着非常好的用户体验。

同时，管理中心的数据可视，移动设备可控。操作性强，审计数据全面，相比传统的企业产品，用户体验要更加流程、优秀。

3.5 典型解决方案

360 天机管理中心部署在企业内网服务器中，是基于 web 的管理系统，可通过浏览器直接访问。天机移动终端可根据控制中心下发的安全策略，进行相应的锁屏、锁定工作区等操作，并可从控制中心服务器下载企业私有应用市场中的应用。控制中心获得移动终端定位等信息时，需要从天机公有云安全服务器中获取相应数据。

部署结构如下图所示：

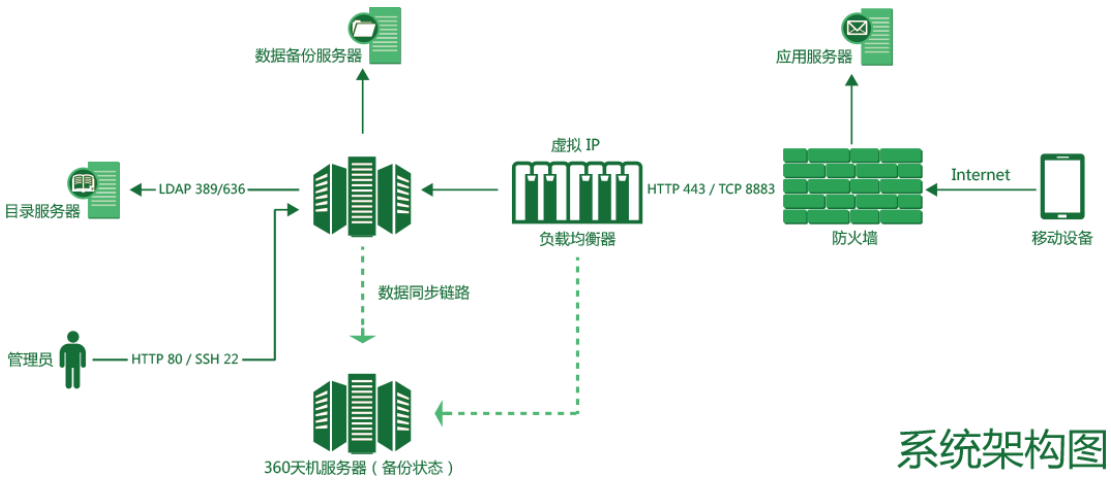

图 6 部署结构图

四 服务支持

方式	服务内容	时间
电话支持	4008 136 360	7X24 小时响应
邮件支持	tianji-kefu@360.cn	24 小时内回复
QQ 支持	122969787/224533511/251755502/183868276	24 小时内回复
论坛支持	http://bbs.360.cn/5500002.html	24 小时内回复
微博支持	http://weibo.com/360wgb	24 小时内回复
远程桌面	通过远程协助解决	24 小时内回复

如需更多专属服务或本地化服务请联系 010-52447412