360 天机移动终端安全管理系统

### Skykey Enterprise Mobility Security Management System

产品白皮书

目录

[一．产品介绍 4](#_bookmark0)

[1.1 移动信息化带来的安全新挑战 4](#_bookmark1)

[1.2 360 天机移动安全管理系统 5](#_bookmark2)

[二．产品定位 6](#_bookmark3)

[三．产品功能架构 7](#_bookmark4)

[四．产品优势 7](#_bookmark5)

[4.1 安全工作区技术 7](#_bookmark6)

[4.2 专属应用市场 8](#_bookmark7)

[4.3 设备强管控技术 9](#_bookmark8)

[4.4 设备准入与罚出 9](#_bookmark9)

[4.5 设备多维度分组 10](#_bookmark10)

[五．产品功能介绍 11](#_bookmark11)

[5.1 用户管理 11](#_bookmark12)

[5.2 设备管理 11](#_bookmark13)

[5.3 应用管理 11](#_bookmark14)

[5.4 安全策略 12](#_bookmark15)

[5.5 终端配置管理 13](#_bookmark16)

[5.6 日志及可视化数据 13](#_bookmark17)

[5.7 运维管理 14](#_bookmark18)

[六．部署及网络架构 14](#_bookmark19)

[6.1 部署逻辑架构图 14](#_bookmark20)

[6.2 网络环境准备 15](#_bookmark21)

[6.3 服务器环境准备 15](#_bookmark22)

[七．实际案例 16](#_bookmark23)

[7.1 某省检察院 16](#_bookmark24)

[7.2 某省政府 17](#_bookmark25)

[7.3 北京市急救中心 18](#_bookmark26)

[附录 A：版权声明 20](#_bookmark27)

[附录 B：免责条款 21](#_bookmark28)

**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 事业单位。众多企事业单位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。这类被称为企事业单位移动终端管 理的现象为企事业单位带来了全新的机遇：

 **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，为企事业单位节约了大量的 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。

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。

# 一．产品介绍

## 1.1 移动信息化带来的安全新挑战

移动信息化趋势为政府和企业带来了机遇，同时也为企事业单位信息安全和管理带来了 新的挑战：

####  打破了传统企事业单位网络边界

企事业单位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事业单位网络边界，正是这种边界的模糊性 使移动终端成为企事业单位信息安全体系的薄弱环节，移动终端中的企事业单位数据也会因 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事业单位数据安全。

####  移动设备具有易失性，从而具有泄露企事业单位数据的隐患

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事业单位敏感数据也因此面临泄密风险。2013 年发布 的关于企事业单位中移动终端办公的趋势调查报告显示，50%的受访企事业单位表示曾经 丢失过储存企事业单位重要数据的设备，其中 23%的企事业单位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事业单位网 络的跳板。

####  员工主动泄密，给企事业单位带来数据泄露的损失

根据调查，尽管 85%的企事业单位采取了保密措施，但仍有 23% 的企事业单位发生 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 拷贝企事业单位重要信息，从而出卖资料。员工的这些行为，导致企事业单位重要信息无意 或有意泄密，不仅为企事业单位带来财产损失，影响企事业单位的业务运营，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 事业单位面临的另一个挑战。

####  应用质量参差不齐，应用市场安全性堪忧

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，如何保证企事业单 位的内部应用不被伪造、篡改、植入代码为企事业单位带来了挑战。同时，根据相关数据分 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事业单位网络的跳板** 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事业单位内网的跳板。

####  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，又有企事业单位数据和应用，个人应用可以随意访 问、存取企事业单位数据，企事业单位应用同样也会触及到个人数据。如何明确区分并隔离 移动终端上的企事业单位/私人数据与应用，禁止企事业单位数据被个人应用非法上传、共 享和外泄，同时禁止企事业单位应用访问个人数据，尊重移动终端上的私人数据是一个难以 避免的问题。

## 1.2 360 天机移动安全管理系统

360 天机移动终端安全管理系统（以下简称“360 天机”）是网神信息技术（北京）股 份有限公司基于移动终端安全所发布的一套面向企事业单位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网神多年来在安全领域的技术积累，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。

# 二．产品定位

360 天机致力于解决企事业单位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，帮助企事业单位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 天机解决了企事业单位移动办公过程中的安全问题，使得企事业单位更安全地推行 移动信息化，企事业单位不用再担心移动终端受到木马病毒的威胁从而泄露企事业单位数据 的问题、移动终端丢失或者被窃而导致的企事业单位数据泄露问题、移动终端成为入侵企事 业单位网络的渠道问题、以及员工恶意泄密问题。

360 天机解决了企事业单位移动办公过程中的管理问题，企事业单位管理员可以更加高 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 天机使得企事业单位员工在享受移动终端办公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。360 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事业单位数据的安全，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。

# 三．产品功能架构

360 天机主要功能包含用户管理、设备管理、应用管理、安全策略、终端配置、安全防 护、日志报表等七类模块。每一模块下细分功能如图 1：



图 1

# 四．产品优势

## 4.1 安全工作区技术

360 天机产品采用新一代沙箱技术，为企事业单位构建一个安全的工作区。在这个工作 区里，创造了一个工作的统一入口，个人生活区域同办公区域可方便灵活切换，只需轻轻点 击安全办公区图标就可轻松、方便进入到办公专属的区域。

在安全办公区中提供了完整的办公套件，可以满足员工基本的办公要求，且运行在 360 天机的安全工作区内的应用数据以及内部的重要数据全部采用高强度的加密方式进行加密 存储，从而保证了专属的安全办公区的数据的安全性，在工作区内禁止了复制、粘贴的功能， 保证个人去有风险的数据无法进入到安全工作区，安全工作区的办公数据无法流出到个人 区。

安全工作区基于的 360 新一代沙箱技术是一项基于应用层实现的数据安全和防护技术，

通过背靠背应用封装流程，对 APK 安装文件逆向，修改或注入沙箱服务代码，为应用提供

沙箱多种安全特性：

数据加密

数据隔离：隔离个人区入口、限制应用程序内打开

数据清除：违规自动清除、远程清除 该技术不破坏程序本身，采用“在应用外边包一层壳” 的方式，隔离个人与企业数据，并 提供加密存储保证企业数据安全。具有兼容性好，可远程动态升级等优点。



## 4.2 专属应用市场



360 天机为企事业单位打造了一个内部专属的应用商店，企事业单位内部应用可完全摆 脱掉以往依靠公共的应用商店进行分发的局面。这样不仅可提高应用发布的效率，同时也提 高了应用发布的安全性，内部专属的应用从上架、更新到下架全生命周期完全自主可控。

360 天机可提供 Android 应用、iOS 应用的发布。



## 4.3 设备强管控技术

针对企事业单位有所有权的设备，360 天机通过和设备厂商合作签名的方式，使天机客 户端具有 SYSTEM 权限，以实现对安卓设备更高级、更严格的管控与限制，具有强管控权 限的设备可实现以下功能：

对应用程序静默安装卸载、黑白名单控制；

对安卓设备硬件功能的强制管控，例如：摄像头、闪光灯、GPS、麦克风、扬声器、 短信、通话、地理位置、出厂设置等；

对安卓设备传输介质进行强管控，例如：WiFi、GPRS、热点、蓝牙、红外、USB、 SD 卡等；

对安卓设备的远程截屏、监控、重启、关机；

## 4.4 设备准入与罚出

#### 4.5.1 设备准入

设备准入是对客户端的激活限制，管理员通过设置客户端激活必须满足的条件，以防止

外来设备激活，恶意获取企事业单位数据。例如，企事业单位集体采购一批设备，设置条件

需匹配设备的 IMEI 号码才可以激活。

#### 4.5.2NAC 网络控制

360 天机产品与 360 网神 NAC 设备准入产品联动，通过规范接入内网的端点行为，保 障内网数据的安全。如图 2，在设备访问内网时，NAC 服务器会判断设备是否满足安装天 机和设备合规两项条件，满足条件则可以成功访问内网，不满足条件则拒绝访问。同时可对 不同用户设置不同的网络访问权限，以实现企事业单位内网的访问权限控制需求。



图 2

#### 4.5.3 设备罚出

设备罚出是对不合规客户端的检查和惩罚，管理员通过设置客户端的违规行为及惩罚措 施，以防止员工的不合规行为引发企事业单位数据被窃取。例如，管理员设定设备 Root 即 违规，客户端发现设备违规，即阻止进入工作区。

## 4.5 设备多维度分组

天机对设备的分组提供了分组、标签、智能标签三种维度的管理方式，使管理员能更灵

活的对不同设备进行下发策略或应用。

基础的分组形式适用于 LADP 导入的用户会保持其组织架构，也可自定义建立组织架 构，同时支持分组的增删改；标签是在单纯的组织架构分组难以满足特殊性的分类需求时， 管理员通过设置标签关联终端；而智能标签更智能化，只需要设置条件，满足该条件的设备 将自动归入该规则，例如设置“设备型号等于安卓”，则安卓设备激活时，将自动进入该规 则类别。

# 五．产品功能介绍

## 5.1 用户管理

天机支持手动添加、CSV 批量添加和 LDAP 三种导入用户的方式，对导入的用户可进 行邮件或短信邀请注册、分组管理、设置管理员、禁用等操作。即用户从导入、管理和删除 的周期，都可以全权掌控。只有超级管理员和管理员才可以登录管理中心，同时超级管理员 可以添加普通管理员，并赋予普通管理员对用户和功能的管理范围和权限，以满足企事业单 位对分支机构的功能权限限制。

## 5.2 设备管理

设备管理是对设备从激活到注销的周期的管理，为保证对设备的全面管控，管理中心可 以查看设备的硬件/系统信息、无线/移动网络状态、应用安装详情、行为日志、网络流量等 基本信息；还可以通过上报屏幕截图、上报地理位置、上报运行状态等监控设备行为；为防 止设备丢失，可以进行锁定设备、清除工作区数据、恢复出厂设置等操作保护企事业单位数 据不被泄露；方便资产管理，可以对设备进行标记为单位设备、转移用户等；还可以通过工 作区密码下发、更新客户端、推送证书等功能强制设备合规操作。

## 5.3 应用管理

天机通过建立企事业单位应用市场以搭建一个安全、统一、便捷的应用下发通道，不仅 很好的规范了企事业单位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 理员统一管理企事业单位移动应用的效率。

为了保证企事业单位移动应用的安全性，天机采用了应用封装技术，对上传到企事业单

位应用市场的应用进行封装处理，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。对应用安装的情况也可进行统计 查看，如图 4。



图 4

## 5.4 安全策略

管理员可通过安全策略灵活的控制对设备的管控强度，有效的管理企事业单位移动设备 的行为合规性，并可对不同分组的设备执行不同的策略，以满足对不同办公场景的员工的行 为限制。而安全策略主要包含以下内容：

密码管理：设备密码复杂度、工作区密码复杂度；

功能禁用：摄像头、蓝牙、移动网络、Wi-Fi、外联设备、恢复出厂设置；

围栏设置：时间围栏、地理围栏、WLAN 围栏

 隐私策略：上报地理位置、上传短信内容、上传含敏感词的信息内容（短信、微信）；

工作区设置：剪贴板隔离、工作区组件隐藏、启动工作区默认打开应用设置等；

违规检测：Root/越狱、更换 SIM 卡/TF 卡、终端失联、连接到非法 WiFi、设备 有病毒等；

惩罚措施：禁止进入工作区、注销天机、清除单位数据等；

网络访问控制：允许或禁止访问的网络地址；

应用策略：应用安装控制、应用运行控制、应用更新控制、应用卸载控制

其他：浏览器网址过滤、设置允许调用的个人区应用；

## 5.5 终端配置管理

终端配置主要是对终端用户的设备或应用所需的配置进行推送管理。包括 WIFI 配置， 管理配置员工连接 WIFI 的权限和密码；Exchange 配置，管理配置员工邮箱的登录权限和 邮箱配置；浏览器书签配置，统一下发书签至客户端浏览器；证书配置，分组推送证书至客 户端；VPN 配置，统一下发系统级和应用封装级 VPN 的账户、密码、认证服务器地址/端 口至客户端；其他邮件配置，按不同分组、标签、智能标签下发邮件配置信息至客户端；企 业通讯录，将导入服务端的单位通讯录统一下发至客户端；APN 配置，将 APN 信息分别下 发至不同的移动警务终端用户。

## 5.6 日志及可视化数据

360 天机会完整记录管理员在管理中心的操作以及用户在客户端的操作日志，以进行行 为审查。管理中心可通过管理员日志、设备日志、事件日志的维度查询日志，并支持按照时 间段和功能分类的进行查找，对重要日志可进行导出文件。

为了方便重点事件的及时查看，管理中心首页会将设备违规情况、策略执行情况、最新 激活设备等重要数据可视化，以柱形图等形式直观显示，管理员可自定义需要显示的图标数 据，如图 5。



图 5

## 5.7 运维管理

管理员可在管理中心进行系统数据的备份和还原，以防止服务器损坏或更换时数据丢 失；同时，管理员也可自主升级天机系统和进行服务器迁移，简化了运维成本。

# 六．部署及网络架构

## 6.1 部署逻辑架构图



### 360 天机服务部部署模式可支持单机部署，也可支持双机热备，同时还可以 支持大型的集群部署的方式，可根据企事业单位的实际场景需求和业务需要，我 们提供灵活的部署方式。

## 6.2 网络环境准备

### 核心服务器需要部署在企业的 DMZ 区域或外网环境，拥有独立的、公网可访 问的域名及 IP 地址，以便客户端通过公共网络连接到服务器端。

**防火墙策略**

### 如天机管理服务器部署在 DMZ 区域，需要在防火墙开放端口，配置策略如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **端口号/****协议** | **源地址** | **目的****地址** | **用途** |
| 443（TCP） | 移动终端 | 管理服务器 | 客户端连接服务器，进行信息上报和策略下发 |
| 80（TCP） | 内网管理员主机 | 管理服务器 | 管理员登录服务器控制台进行信息查看或策略配置 |
| 8883（TCP） | 移动终端 | 管理服务器 | 消息推送和下发服务 |
| 22（TCP） | 内网主机 | 管理服务器 | 管理员登录后台系统进行系统调试 |
| 53（TPC/UDP） | 管理服务器 | DNS服务器 | 访问内网 DNS 服务器，进行域名解析 |
| 123(TCP/UDP) | 管理服务器 | NTP服务器 | 访问内网 NTP 服务器，进行时间同步 |

## 6.3 服务器环境准备

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **建议服****务器类型** | **建议处****理器核心** | **建****议内存** | **建****议存储** | **可管理终****端数量** | **可支****持并发** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 虚拟机/物理机 | 4 | 24G | 320G | 10000~12000 | 1000~2000 |
| 虚拟机/物理机 | 8 | 32G | 320G | 20000~25000 | 4000~5000 |
| 物理机 | 8 | 48G | 500G | 50000 | 6000-7000 |
| 物理机 | 16 | 64G | 500G | 100000 | 8000~9000 |

# 七．实际案例

## 7.1 某省检察院

2016 年 9 月，高检院印发实施《“十三五”时期科技强检规划纲要》，明确了“十三五” 时期“智慧检务”建设的时间表和路线图，明确了“十三五”时期要加强综合管理应用，完 善办公信息系统和档案管理系统，并推广移动办公应用。

随着“十三五”期间“智慧检务”平台建设的深入及移动终端技术的迅速发展，某省检 察院涌现了大批的移动办公应用，业务覆盖范围包括公文传阅、公文办理、会议室申请、文 件检索、历史文件查询等，检务人员在日常工作中使用移动终端办公的频率越来越高，但这 些包含大量内部数据和机要文件的应用大都直接安装在检务工作人员的私人手机里，与私人 数据一样无加密的存储在手机上，移动信息化安全管理显得非常滞后，主要表现在以下几个 方面：

（1） 对接入网络的日益增多的移动设备状态无法监管：移动接入的场景多种多 样，无法保障安全，包括 3G/4G、家用 WiFi、公用 WiFi 等。设备本身是 否已被感染病毒，设备使用者身份不得而知等。

（2） 各种敏感信息在移动端处于无控制状态：没有安全的数据存储区、文档管 理器和邮件客户端来保障文件及邮件内的数据，用户可以将内部文档或邮 件附件通过手机上的第三方软件随意转发或保存，引起潜在的数据泄露风 险。

（3） 移动应用缺乏统一管理：众多的移动应用，安装下载升级没有统一管理。

移动应用无防范病毒木马、恶意广告等的措施。

经过对 XX 检察院移动办公需求的深入研究，360 移动安全产品部凭借丰富的公检法司 行业实践经验，成熟可靠的产品以及完善的本地化服务和支持网络，为广西全区检察院提供 了一套完整的移动安全解决方案。

 360 天机为 XX 检察院打造了一个办公统一入口，使用沙箱技术，建立了一个安全 工作区，与个人区隔离，保障办公区数据的安全；

 其次，天机与 XX 检察院现有 VSWITCH 对接 360VPN，通过 360ID+VPN 认证 的方式，保障进入检察院内网系统内人员身份的安全；

 再次，天机为 XX 检察院建立了一个统一的专属应用市场，统一进行应用全生命周 期管理。

## 7.2 某省政府

某省发布的大数据产业发展应用规划纲要(2014-2020 年)提出，将组织实施重大应用 示范项目，推动建设面向政府、公众和企事业单位的云计算和大数据服务平台，建设“七朵 云”。电子政务云工程作为“七朵云”之一，将力争在 2014-15 年取得重大突破。其主要任 务是以省市县三级协同办以系统为基础，基于云计算的电子政务外网平台顶层设计，建立统 一的省电子政务云平台。实现全省“省市县”地方三级政府，20 万公务员协同办公系统建， 加强省政府办公厅与各级各部门的互联互通和非涉密文件网上流转，大量减少部门往返办公 厅取件现象，提高了公文运转和会议通知效率，降低行政成本。

因为整个项目并非省内统一采购设备，全省 20 万公务员移动终端碎片程度非常高，且 网络覆盖三大运营商，天机平台的稳定性和兼容性保证绝大多数移动终端可以正常管控。为 用户提供的服务如下

APP 的快捷部署和升级

预防手机病毒和木马

避免终端失窃而导致的数据泄露

个人数据与办公数据隔离

## 7.3 北京市急救中心

#### 背景描述：

 北京急救中心负责北京 120 急救网络规划和管理。按照市政府的要求，根据区域面积、

 人口分布、急救需求等情况设置了 75 个急救网点，10 个远郊区县设立急救分中心，缩短

 了急救半径。提高了急救呼救满足率。同时也带来了采用移动办公方式存在的安全问题、工

作同步问题。

#### 客户问题：

 移动终端分散，无法集中、统一管理

 中心派发移动设备，得不到专机专用

 终端丢失，患者信息无法保证安全性

在 360 天机的帮助下，北京急救中心实现了以下功能：

对所有平板电脑设备进行统一注册和管理，设备信息统一呈现。

建立自己的应用商店，所有内部 APP 均可以第一时间通过该应用商店推送给所有 的平板电脑，实现 APP 应用的统一下载、安装和更新。

禁止医护人员安装与工作无关的应用，实现应用的黑白名单。

对内部 APP 进行加固封装，确保 APP 应用本身的安全，防止被反编译和二次伪造 盗版，封装确保 APP 应用数据加密、公私数据互访隔离。

 通过移动沙盒技术形成独立的办公工作区，运行或存储在该工作区的数据均经过加

密，保证平板电脑上的数据安全。

对终端和应用进行木马扫描，确保终端和整个内网环境的安全，同时避免平板电脑 被攻击者当作攻击医院内网的跳板。

# 附录 A：版权声明

《360 天机移动终端安全管理系统产品白皮书》为网神信息技术（北京）股份有限公司 版权所有，并保留对本文档及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特 别注明外，其著作权或其他相关权利均属于网神信息技术（北京）股份有限公司。未经网神 信息技术（北京）股份有限公司书面同意，任何人不得以任何方式或形式对本手册内的任何 部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

# 附录 B：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。 网神信息技术（北京）股份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，但网神信息技术（北京）股份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。