|  |
| --- |
| **EONS企业移动安全管理平台**  **产品白皮书V4.0** |



|  |
| --- |
| 版本：4.0 © 2018启迪思创 |

**目 录**

[1. 概述 4](#_Toc519187702)

[1.1 背景 4](#_Toc519187703)

[1.1.1 移动信息化成为趋势 4](#_Toc519187704)

[1.1.2 移动终端市场的高速增长 5](#_Toc519187705)

[1.1.3 主流智能操作系统继续强化其企业特性 6](#_Toc519187706)

[1.1.4 国内移动信息化在各行业遍地开花 6](#_Toc519187707)

[1.2 移动信息化安全现状 7](#_Toc519187708)

[1.2.1 个人与工作场景混合导致的隐私及数据安全问题 7](#_Toc519187709)

[1.2.2 移动化安全良莠不齐 7](#_Toc519187710)

[1.2.3 移动端碎片化特征以及快速迭代导致的管理难题 8](#_Toc519187711)

[1.2.4 消息推送乱象 8](#_Toc519187712)

[1.2.5 安全认证和用户体验的矛盾 8](#_Toc519187713)

[1.3 EONS企业移动安全管理平台概述 9](#_Toc519187714)

[1.4 平台架构 9](#_Toc519187715)

[1.4.1 系统架构 9](#_Toc519187716)

[1.4.2 平台逻辑架构 11](#_Toc519187717)

[1.4.3 网络部署架构 11](#_Toc519187718)

[1.5 EONS企业移动安全管理平台功能 12](#_Toc519187719)

[1.5.1 移动虚拟隔离（M-VirtualSpace） 12](#_Toc519187720)

[1.5.2 移动安全桌面（M-Desktop） 12](#_Toc519187721)

[1.5.3 移动安全接入（M-Tunnel） 13](#_Toc519187722)

[1.5.4 移动应用套件（M-WorkSuites） 13](#_Toc519187723)

[1.5.5 移动终端管理（M-EMM） 15](#_Toc519187724)

[1.5.6 终端病毒查杀 17](#_Toc519187725)

[1.5.7 用户中心 17](#_Toc519187726)

[1.5.8 认证中心 18](#_Toc519187727)

[1.5.9 消息中心 18](#_Toc519187728)

[1.5.10 数据统计 18](#_Toc519187729)

[1.5.11 日志管理 19](#_Toc519187730)

[1.5.12 权限管理 20](#_Toc519187731)

[1.6 移动应用加固平台 20](#_Toc519187732)

[2. 功能优势 21](#_Toc519187733)

[2.1 全面的移动终端安全防护方案 21](#_Toc519187734)

[2.1.1 移动虚拟空间（VirtualSpace） 21](#_Toc519187735)

[2.1.2 安全工作桌面 21](#_Toc519187736)

[2.1.3 数据防泄漏 22](#_Toc519187737)

[2.1.4 全面的通道加密技术 22](#_Toc519187738)

[2.2 开放的API架构 23](#_Toc519187739)

[2.3 硬件一体化 24](#_Toc519187740)

[2.4 跨平台的多功能一体化移动管理方案 24](#_Toc519187741)

[2.5 绝佳的移动使用体验，同时兼顾个人隐私保护 25](#_Toc519187742)

[3. 行业方案 26](#_Toc519187743)

[3.1 医疗方案 26](#_Toc519187744)

[3.2 政府方案(1) 27](#_Toc519187745)

[3.3 政府方案（2） 27](#_Toc519187746)

[3.4 金融方案 28](#_Toc519187747)

[4. 客户价值 30](#_Toc519187748)

# 概述

## 背景

### 移动信息化成为趋势

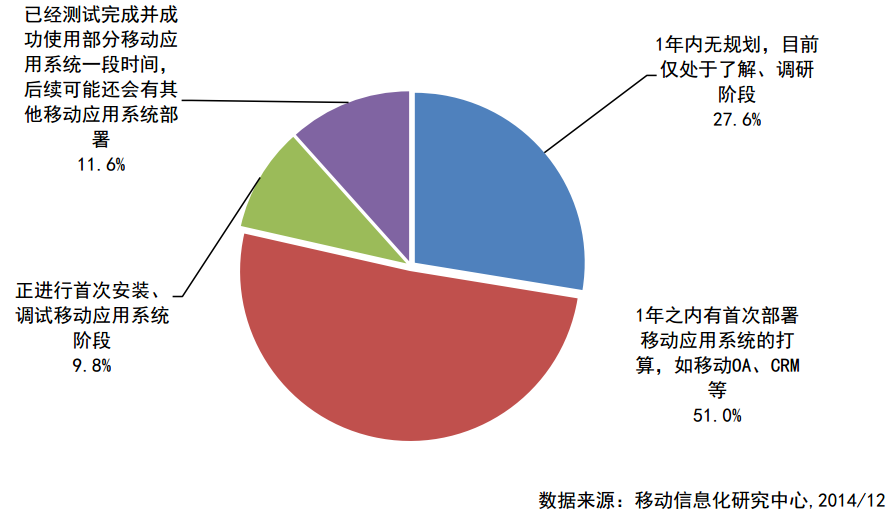
随着互联网无线通信和终端技术的飞速发展，移动终端在改变人们生活方式的同时，也深刻影响着人们的工作方式。工作不再局限在办公室内，人员可以随时随地进行移动办公，员工可以自由分配碎片化的时间进行高效率的工作，从而更及时的处理工作事务，提升工作效率，另外移动办公可以让企业在业务上有了更多的创新模式，从而显著提高企业经营效率，提升客户和合作伙伴的满意度。根据Gartner分析报告，2016年将会有46%的组织彻底使用移动设备办公，另外CNNIC统计，截至2014年12月，我国手机网民规模达5亿多，2015年3月，我国手机网民规模已经超6亿。

万人

统计来源：CNNIC中国互联网络发展状况统计调查 2014.12

伴随移动互联网的迅速发展，移动信息化业务自然遍地开花，通过手机、PDA等掌上

移动终端，以及电信、互联网通讯技术融合的方式，使得各级政府、企业、个人的信息化应用保证你可以随时随地进行移动化的工作、学习和娱乐。移动应用的价值开始在各行业的实践中突显，相关的应用部署条件逐步开始成熟，并且企业用户内外部业务需求的发展对信息交互的及时性要求越来越高，这些诸多因素都促使更多的企业用户开始对移动信息化产生兴趣。以下是2014年行业客户对移动信息化建设的统计，



由图可看出，移动信息化建设仍有很大的市场空间。

移动信息化已经成为企业用户在信息化领域创新的主要方向。信息安全厂商已经意识到移动互联网信息安全以及用户隐私保护的广阔前景，并加大了技术、产品研发力度。目前移动安全市场一直保持着高速的增长态势。2013年中国移动信息安全市场规模达到7.37亿元，同比增长68.3%，预测2016年市场规模将达到32.46亿元。

### 移动终端市场的高速增长

根据IDC2014年给出的预测来看，全球范围内，移动终端市场仍然呈现高速增长的态势，国内智能终端的增速超过了30%。远远超过全球平均增速。



### 主流智能操作系统继续强化其企业特性

当前移动互联网时代，主流的操作系统为Android，iOS，WP。Android作为全球最普及的移动操作系统越来越成为企业移动信息化的主力平台，而且Android也越来越重视其在企业应用场景中的属性，2014年推出了Android for Work就是Google针对Android更好的用户移动办公的全新的解决方案，这充分说明了Google对于企业市场的重视。而iOS作为全球最受欢迎的操作系统，一直非常重视企业市场，很早就推出了针对教育和企业市场的解决方案。而Windows Phone虽然在移动互联网时代落后于Android和iOS两大操作系统，但是由于其在PC时代积累的企业客户以及Windows 10的及时推出更多的企业级安全属性，使得Windows系统在企业级移动市场的机会也出现转机，再加上Windows系统对PC+移动统一终端管理方案的天然优势。

### 国内移动信息化在各行业遍地开花

在国内，企业移动信息化在各行业正在如火如荼的开展，首当其冲的是金融，证券，保险，纷纷推出了类似于移动开卡，移动投保，移动微贷等业务，其次，政府部门移动信息化需求主要集中在移动执法，移动审批，移动OA等方面，另外在电力，教育，物流，零售，医疗等行业，移动信息化均有着比较广泛的应用。



## 移动信息化安全现状

企业在开展移动信息化的过程中，由于企业及个人数据同时存储在同一款移动终端上，所以会导致高价值的企业信息资产暴露在公共互联网之外，从而导致企业面临众多的安全问题，总结来说，有以下三点。

### 个人与工作场景混合导致的隐私及数据安全问题

移动办公时代的移动终端，通常即会作为办公终端，也同时会作为个人终端使用，这样就会导致企业数据资产和个人的信息混合存储在一起，这种情况带来两类问题，一类是由于企业需要对企业的移动终端及应用进行管理，势必要导致企业在管理终端，企业应用及数据时影响到员工的个人隐私，另外一类问题是因为企业的数据存储在具有一部分个人属性的移动终端上，会导致企业核心数据资产出现被泄露的风险。因为在移动终端上，我们只需要点击几下就能下载各类应用，而移动恶意软件常常通过伪装成正常应用，或者二次打包成热门软件，通过应用市场、手机论坛、二维码等多种渠道传播。一旦它们被安装在用于移动办公的智能终端上，就很可能侵入企业的办公系统和生产系统，窃取企业的机密数据，对企业造成重大损失。

### 移动化安全良莠不齐

企业移动化，往往是从某个具体的应用开始，其具体的安全需求均是以这个应用来进行衍生，随着需求的增加，移动化应用也会不断增加，不同的应用，不同的开发厂家，必然造成应用安全能力不一致，如何统一应用安全标准，如何保证每个应用更新升级都是满足统一的安全基线，成为企业安全的头疼问题。

### 移动端碎片化特征以及快速迭代导致的管理难题

企业移动办公面临的另一大问题是移动平台的碎片化，多样化以及快速迭代特性给企业管理带来的复杂度和成本的激增，在原有的PC互联网时代，企业要进行办公，通常会配置统一的标配机、标准化的操作系统和软件，IT部门不必为管理设备花费太多精力。但是在移动互联网时代，移动智能终端呈现百花齐放的景象，除了终端品牌，机型众多之外，移动操作系统也由原来的微软一家独大，变成了Android，iOS，WP三大操作系统厂商割据市场的局面，另外移动系统天然具有更新频率快，碎片化的特征。所有这些因素叠加，导致企业IT的管理难度和管理成本出现了几何式的增加。

### 消息推送乱象

为了保证应用随时都能接收消息、指令，每个应用都希望自己在用户手机中一直保持运行状态，才能及时的接收信息指令。因此，很多应用都会通过进程守护、应用互拉等方式保证自己进程的存活，此类似应用数量一旦过多，必然造成终端设备耗电增加，用户体验降低。有什么办法既能保证应用都能及时收到消息指令，又能对终端的耗电降至最低？

### 安全认证和用户体验的矛盾

在原有的PC时代，以账号密码的输入作为最基本的认证已经被人们所接受。在移动端，仍然面临着安全的认证，考虑到手机、pad的输入键盘和PC机的键盘输入差异性，一个应用的输入认证可以接受，超过三个应用的账号密码输入，自然就会出现反感情绪，尤其是复杂的密码。这样，指纹认证、人脸识别、声纹识别等认证方式出现，解决了输入的繁琐，移动端的单点登录解决了反复认证的烦恼。但如何确认这些移动端的快捷认证是安全的？

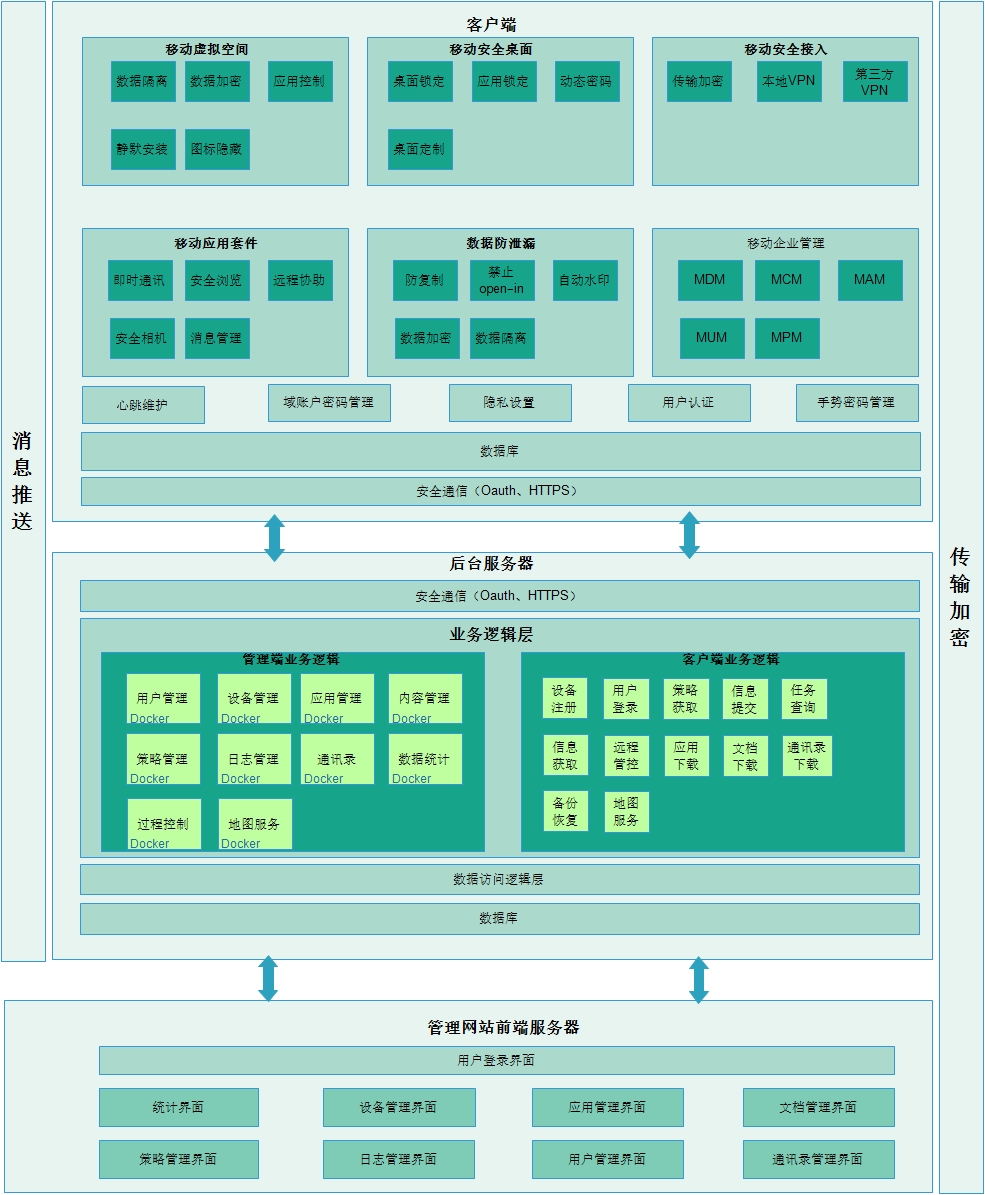
## EONS企业移动安全管理平台概述

启迪EONS企业移动安全管理平台（简称：EONS MSP），是一套实现企业智能终端安全管理的跨平台解决方案。该平台从端、管、云、智四个部分入手，端：以专用终端和个人终端划分，提供移动安全桌面（M-Desktop）、移动虚拟空间（M-VirtualSpace）、移动应用套件（M-WorkSuites）；管：容器级安全接入，为企业应用提供数据安全通道；云：以云为基础，划分移动安全管理中心、移动安全中心、移动认证中心、移动消息中心、移动用户中心等多个中心，智：安全态势感知，让终端安全可视化、实时事件展示、终端安全评级。为用户建立移动安全基础服务平台，为企业移动信息化提供一站式安全解决方案。

## 平台架构

### 系统架构

启迪EONS企业启动安全管理平台整体架构如图所示，总体来说分为“客户端”和“服务器端”两部分，其中：客户端包含Android客户端和iOS客户端；服务器端包含管理网站前端系统、数据处理系统、消息推送系统、数据库系统、安全接入系统五个子系统。



管理网站前端系统:接受web管理请求，实现所有管理功能web界面化。

数据处理系统：移动安全管理平台处理中心，提供认证、授权、策略、管理、日志等一系列处理工作。

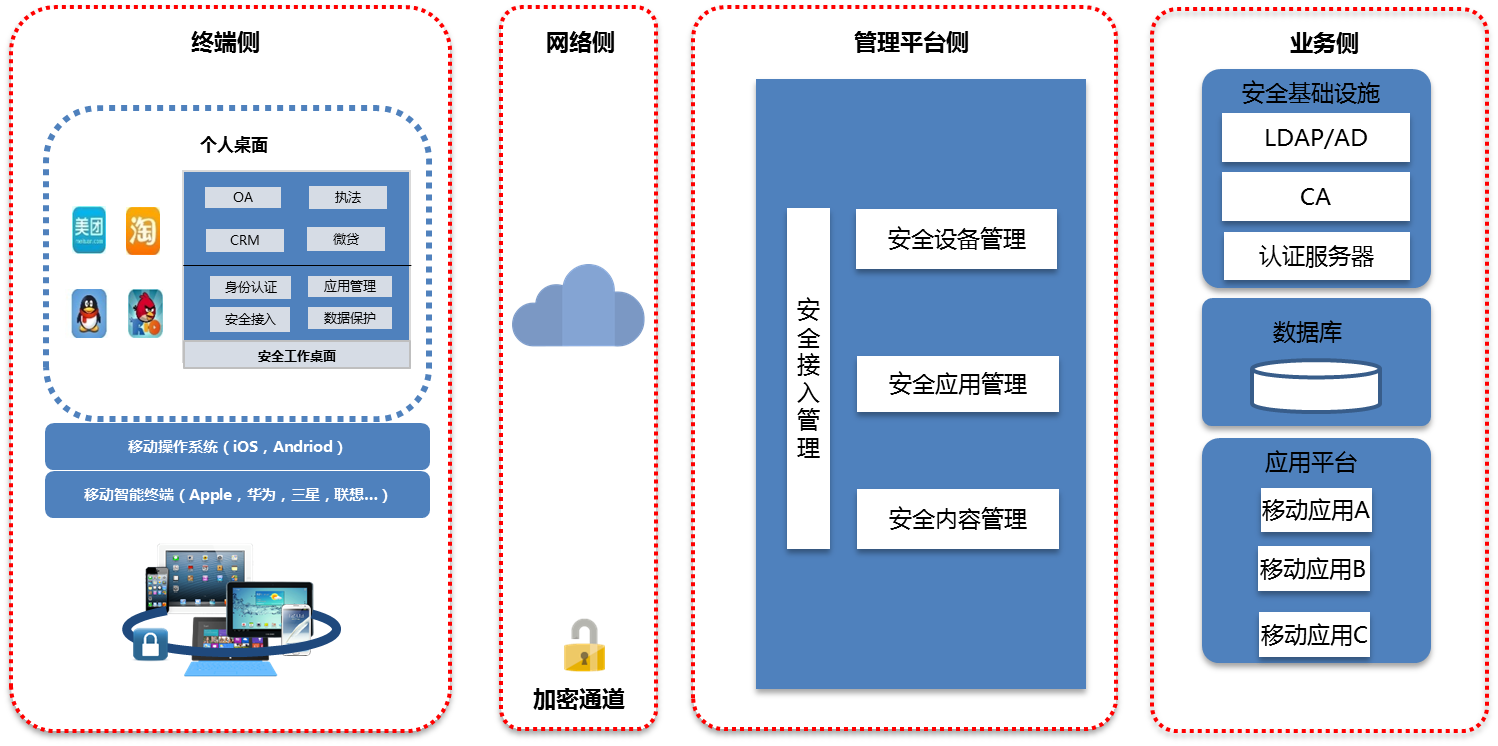
数据库系统：设备信息、管理信息、用户信息等数据存储

消息推送：提供管理平台到移动设备的策略下发、消息推送能力

安全接入系统：提供移动终端到服务端、管理PC到服务端、推送服务器到移动终端数据加密处理English。

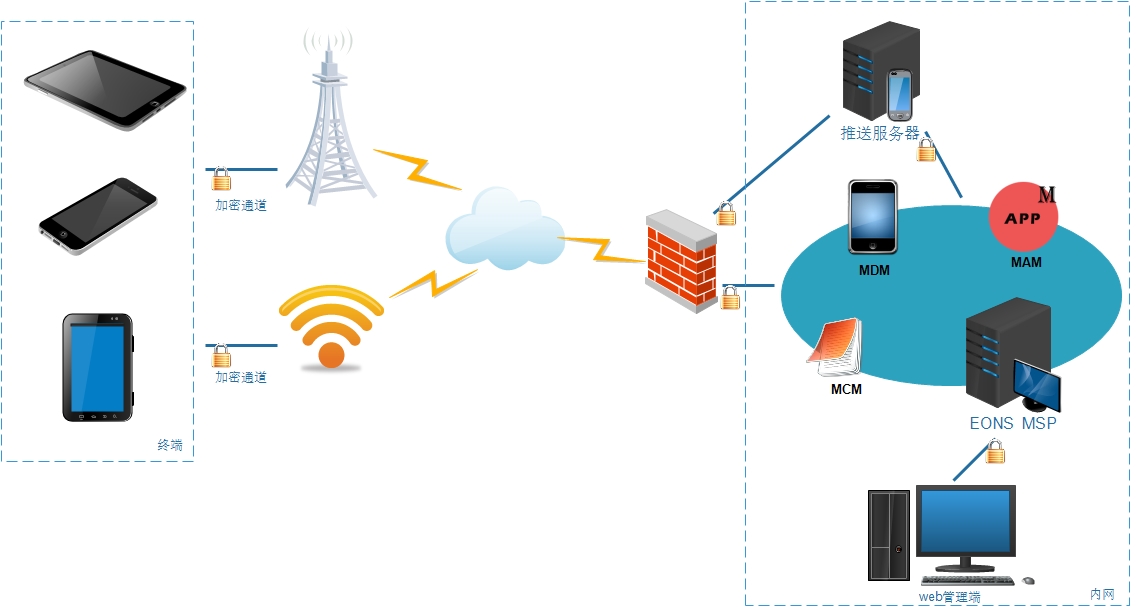
### 平台逻辑架构

分为终端、网络、EONS平台和业务4层关系。终端有MSP客户端实现安全保护，网络使用传输加密，EONS平台实现设备、应用、内容、策略、统计等管理功能。



### 网络部署架构

启迪EONS企业移动安全管理系统在企业网络系统中的部署位置处于内网与外网之间的DMZ区，或者是企业内网，旁路部署即可。



## EONS企业移动安全管理平台功能

### 移动虚拟隔离（M-VirtualSpace）

采用移动虚拟化技术，在移动终端建立一个虚拟的安全工作区，实现数据的隔离、数据加密、应用控制等安全功能。第三方应用无需集成SDK或wrapping，即可实现数据安全隔离、应用控制等功能。

1. 数据隔离

实现虚拟空间内应用图标隐藏（仅显示在安全工作区）、应用安装目录重定向。

1. 应用静默安装卸载
2. 应用控制

实现应用启用禁用

#### 安全容器

以SDK集成方式实现第三方应用逻辑安全隔离。

1. 第三方应用数据加密

以SDK方式，实现对第三方应用所有产生的所有数据进行加密

1. 应用数据加密算法

支持国密（SM2、SM4）和AES加密算法

1. 数据隔离

应用图标隐藏、复制剪切控制、open-in控制

1. 应用控制

应用启停、应用数据清除、应用使用移动数据、wifi网络、蓝牙的控制

### 移动安全桌面（M-Desktop）

一个只有工作的安全桌面，锁定应用，强制进入，无法退出。定制一个你想要的安全工作桌面。

1. 安全桌面

安全桌面的应用无法退出到主屏幕，只能工作在自己的界面，桌面应用内容可自主定制。

1. 应用锁定

锁定应用在当前屏幕，无法退出，即使重启也无法退出，可多个应用之前切换。

1. 桌面背景定制

可以后台定制客户端显示的背景图片和显示文字

1. 退出审批

提供退出审批功能，用户可以提出申请，管理员审批。

1. 动态密码退出

离线状态依然可以通过动态密码机制退出安全桌面。

### 移动安全接入（M-Tunnel）

对于希望远程接入企业内网的第三方应用，可以通过应用级VPN实现应用对内网业务系统的安全访问。

1. MSP平台自身集成VPN模块，为第三方应用提供VPN服务。
2. 支持全通道和仅合法应用建立VPN通道。
3. 支持内外网自动切换
4. MSP平台提供第三方VPN厂商支持，可直接向第三方应用厂商提供带有VPN厂商接入功能的SDK。

### 移动应用套件（M-WorkSuites）

#### 安全通讯

提供企业内部的安全通讯和通讯录功能

安全通讯是企业内部通讯的安全通讯工具，不同于常见的即时通讯产品，它更注重安全，更注重即时性。

1. 独有的对讲机模式，方便快速喊话
2. 通讯内容本地加密
3. 通讯录管理员定制，不同人分配不同通讯录。且员工不能自己添加通讯人员，保证通讯人员的内部可控。
4. 聊天支持发送文字、语言、文件、照片功能。
5. 支持建立群会话，成员管理。

#### 安全浏览器

安全可控的企业级浏览器，只为企业准备的安全浏览器。

1. 数据加密

支持对浏览器产生的cookies、缓存文件、下载文件实现加密，后台可控。

1. 安全控制

支持禁止URL输入、禁止下载、禁止剪贴板控制功能

1. 隐私保护

支持清除浏览器浏览历史、缓存文件（包括flash文件、表单密码等）、cookie保证隐私不泄漏

1. 书签定制

浏览器的访问链接由用户自己定制，做到绝对的访问黑白名单

1. 专用文件查看

浏览器下载文件后台可控全部加密，文件只能由内部专用阅读器打开

1. 传输加密

集成本地VPN、天融信、深信服的VPN模块，轻松实现安全访问内部web服务。

#### 安全相机

独立研发安全相机应用，自动实现照片视频加解密

#### 远程协助

能够远程查看和控制移动终端，方便IT管理员排查故障、定位问题。

#### 安全邮件

提供移动端的邮件客户端，保证邮件收发的便捷性和安全性。

### 移动终端管理（M-EMM）

#### 设备管理

终端设备与用户信息绑定，做到设备注册、认证、激活、使用、淘汰各个环节的全生命周期管理。管理功能主要如下：

1. 资产管理

设备的归属、资产编号、归属跟踪、设备信息维护、资产导出等功能。

1. 远程控制

设备的淘汰、数据擦除、恢复出厂设置、锁定设备等远程控制功能、消息推送功能，能够向移动设备进行消息推送

设备定位，能够定位设备位置和一段时间内的移动轨迹。

1. 设备配置

能够下发wifi、VPN、APN、邮件等配置，方便用户使用

1. 设备管理状态跟踪

对设备的管理状态过程进行跟踪，管理员可以查看对设备所发起命令的执行阶段、执行状态、执行结果，以及子命令的执行状态。

1. 合规准入

定期检测终端合规状态，并根据违规执行提醒和惩罚措施。

可检测root/越狱、SD卡异常、SIM卡异常、OS系统版本、应用黑白名单、必装应用等状态。

6、时间地理围栏

以时间单元和地理位置区域作为围栏，对进入围栏和离开围栏行为作出不同的处理，如禁用摄像头、禁用网络等，实现时间和地理围栏的管控。

1） 支持围栏内控制锁屏、相机、移动网络、WiFi、安全空间、应用

2） 地理围栏支持不规则多边形区域划分

3） Android能够实现需要root也能对应用进行禁用

#### 应用管理

应用管理即提供企业应用商店功能和应用管理功能，保证应用安全、可靠、可控。主要功能如下：

1. 应用商店

提供iOS企业应用、iTunes应用商店应用、Android企业应用三种方式上传应用，并提供应用的上架、下发、删除等应用全生命周期管理。

1. 应用数据加密

对应用所有数据进行加密处理

1. 应用传输加密

对应用的数据传输进行加密处理

#### 内容管理

企业内部重要文档数据的管理。主要功能包括文档的上传、修改、下发和删除。并在终端实现所有企业文档加密。

1. 支持音频、视频、文档等多种格式的文件
2. 集成独有的文档阅读器、视频和音频播放器
3. 所有文件实现文件加密、数据隔离
4. 支持文档自动水印功能
5. 支持文档泄露追踪功能

#### 安全策略

提供终端管理的一系列安全策略，主要功能如下：

1. 设备策略

设备配置策略

通过管理平台，下发配置策略给终端，如密码、Wifi、VPN、Activesync、APN、凭证等策略

设备限制策略

通过管理平台，下发设备的限制策略、如禁用摄像头等

应用合规策略

通过管理平台，下发应用合规策略

1. 桌面策略

包括桌面锁定、应用锁定、桌面定制、动态密码、退出审批等策略

1. 接入策略

包括本地VPN和第三方VPN策略的配置

1. 安全容器

包括容器策略、应用控制策略、浏览器策略、文档水印策略

#### 用户管理

对使用企业移动管理系统的用户进行管理，主要功能有：

1. 用户管理

用户添加、删除、修改、移动。支持LDAP用户同步导入

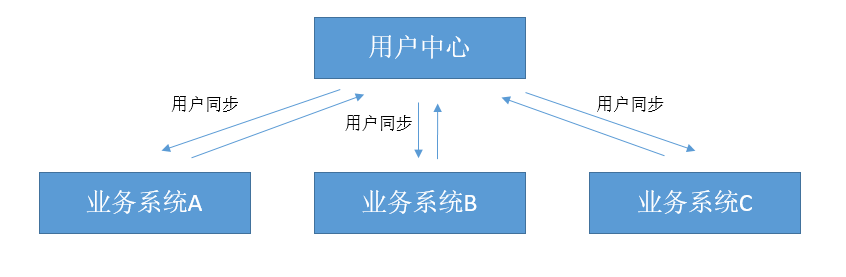
1. 用户组管理
2. 角色管理
3. 添加用户，可批量发送激活邮件

### 终端病毒查杀

MSP内置病毒查杀模块，可检测终端环境安全和扫描风险应用、木马应用、恶意行为、非法证书应用等

### 用户中心

用户中心作为用户数据承载体，可以给不同业务系统提供数据同步功能。它轻松实现了用户账号的统一，也为用户实现单点登录等复杂场景提供便捷通道。



1. 提供标准用户同步接口，供业务系统同步用户
2. 支持主动推送消息，真正意义实现实时同步
3. 支持LDAP/AD数据同步至用户中心

### 认证中心

认证中心为移动业务提供认证接口，建立认证代理服务，实现统一认证。

1. 支持单点登录，一次登录，所有安全空间内应用免登录

### 消息中心

提供可私网部署的消息中心平台，为所有第三方应用提供消息推送能力（支持iOS和Android），第三方应用只需对接此消息中心平台，即可做到消息推送、策略下发、文件下发等，也无需做应用保活，无需做自己的消息推送。

### 数据统计

1. 安全态势感知

以终端安全为基点，图形化展示终端的安全态势，为用户提供安全分析、数据分析可视化平台。

1） 以图表的形式，展示终端安全的整体情况，帮助用户直观的、全面的去分析的终端安全形式。支持全球、中国以及省级的切换

2） 根据用户选择，可实时显示终端的信息：设备名、使用者、安全等级、平台版本号、安全客户端版本号、更新时间、电池电量、内外存储容量、连接的网络目录快捷方式，可以为目录创建快捷方式，用户直接从MSP桌面打开目录查看文件

3） 实时显示最近的终端告警事件

1. 提供以下数据统计：

设备数统计

应用数统计

用户统计

在线设备统计

设备平台统计

设备归属统计

越狱统计

策略统计

管理状态统计

版本统计

应用类型统计

离线统计

违规统计

上线统计

### 日志管理

管理员操作日志：记录管理员的登录、创建、修改、删除、分配等所有操作记录。

用户日志：记录用户设备合规告警信息，包括：

1、锁屏密码不合规告警

2、SD卡不合规告警

3、SIM卡不合规告警

4、应用黑白名单不合规告警

5、必装应用不合规告警

6、系统版本不合规告警

7、离线时长不合规告警

8、root/越狱告警

### 权限管理

1. 分权管理

管理员默认分为安全管理员、系统管理员和审计管理员。三个管理员权限分离，互相制约。实现管理员的三权分立。

1. 分级管理

管理员可以创建多个下级管理员，可以为管理员分配不同的权限和管理范围。从而实现MSP平台的分级分布式的管理。

## 移动应用加固平台

通过移动应用加固平台，为应用提供对应安全特性：数据加密、安全隔离、功能限制、WIFI管理等功能。

数据加密，支持全盘加密及制定文件加密。加密格式支持docx、xlsx、pptx、doc、xls、ppt、txt、pdf等格式。并支持文件隐藏功能。

安全隔离，支持图标隐藏、禁止截屏、录屏、剪切板控制、分享控制功能。

功能限制，支持禁止开启摄像头、蓝牙、录音、邮件客户端、移动数据控制等。

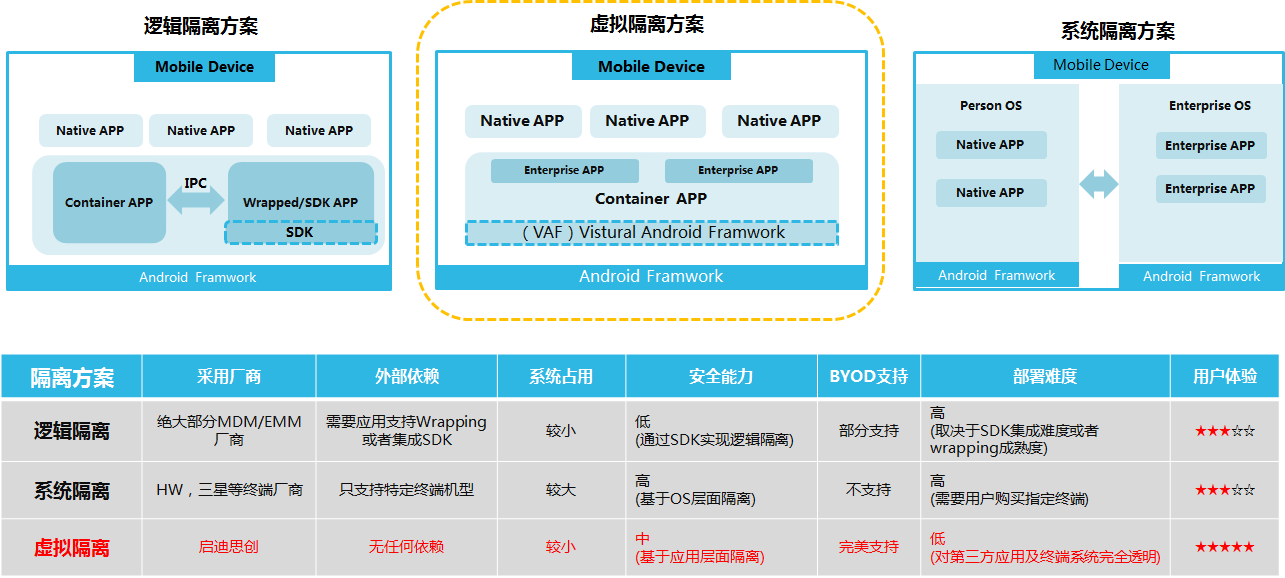
Wifi管理，支持wifi黑白名单功能。禁止wifi网络功能。

# 功能优势

## 全面的移动终端安全防护方案

### 移动虚拟空间（VirtualSpace）

启迪独创的移动虚拟空间技术，采用虚拟化技术，实现移动终端数据的安全隔离、数据加密及各种安全管控功能。无需第三方应用做任何修改，即可实现安全隔离功能。以下是移动虚拟空间跟移动端各种隔离技术的对比：



### 安全工作桌面

通过策略定制一个你想要的工作桌面。防退出功能让安全工作桌面退出无死角，只有合法授权才能成功退出。类手机桌面的软件解密，操作无障碍，桌面图标任意拖动，背景可定制。同时支持Android和iOS安全桌面



### 数据防泄漏

EONS MSP拥有一整套数据防泄漏方案来确保移动终端的数据隐私性安全性。

所有企业相关数据进行数据加密，并能控制剪贴板，防止拷贝粘贴。

专用文档阅读器，加密office文档只有MSP内专用文档阅读器可以打开使用。支持word、pdf等90%以上office文档格式。

专用音视频播放器，加密的音视频文件只有MSP内专用的音视频播放器才可以播放使用。支持rmvb、avi、mp3等90%以上音视频文件

专用相机，提供专用的相机程序，自动实现照片和视频的加解密。

专用浏览器，提供专用安全浏览器，实现对浏览器产生数据自动加密，并可定期清除浏览器隐私信息。

自动水印，对机密文档实现自动添加水印

泄露追踪，可根据特有的字符追溯泄露文档的使用者。

### 全面的通道加密技术

平台集成VPN功能，可以保证终端数据在链路传输是安全的。如图所示，无论是终端到企业内网、终端到管理平台、管理平台至推送服务器、web管理端至管理平台，均采用加密。真正做到通道加密无死角。



## 开放的API架构

EONS MSP产品整个平台功能接口化，可以快速方便的与第三方集成。目前整个平台开放多达150个API接口，可以满足移动安全的绝大多数安全需求。目前提供的接口主要分为以下几类：

设备管理

应用管理

内容管理

用户管理

通讯录管理

安全接入管理

安全桌面管理

安全容器管理

## 硬件一体化

硬件一体机（简称：MSP-H），是一套基于移动化场景的移动安全快速部署、简单操作的整体解决方案。MSP-H集成企业终端管理（EMM）、移动数据安全隔离、移动数据防泄漏（DLP）、移动安全接入、移动安全桌面、即时通讯、安全浏览等不同的安全模块的同时，划分不同的硬件配置和性能档次，更精准的满足用户移动安全需求。最终为企业移动化提供多元化的解决方案。其主要特点如下：

 功能一体化：集所有功能为一体的硬件一体机

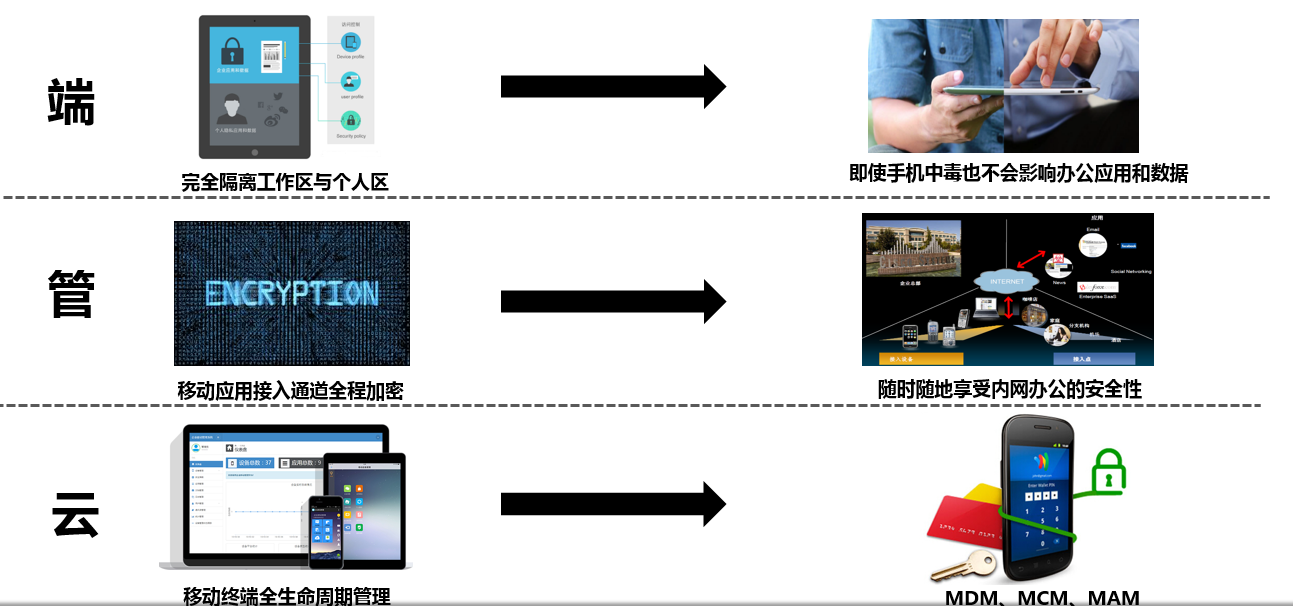
 快速部署：界面化配置网络、时间、系统维护，轻松实现上架部署使用

 操作简单：一键配置备份、数据备份、一键升级

 安全保障：高性能配置、磁盘镜像、冗余电源

## 跨平台的多功能一体化移动管理方案

EONS移动安全管理平台对终端的安全管理，是基于应用层，不会因设备厂商的不同导致功能不可用，并且同时支持android、iOS两大系统最新版本，从而满足用户设备采购和BYOD应用场景的需求。同时结合了设备管理、应用管理、内容管理等多个核心管理功能，提供给用户一整套安全解决方案。



## 绝佳的移动使用体验，同时兼顾个人隐私保护

* 原生体验

提供原生桌面使用风格，个人无任何学习和适应成本。

* 公私分明

工作进入安全空间，生活娱乐返回个人桌面，互不干扰。

* 隐私保护

安全策略完全基于移动虚拟空间，对个人无关信息不做收集，同时BYOD用户可进行网络、位置等个性化隐私设置。



# 行业方案

## 医疗方案

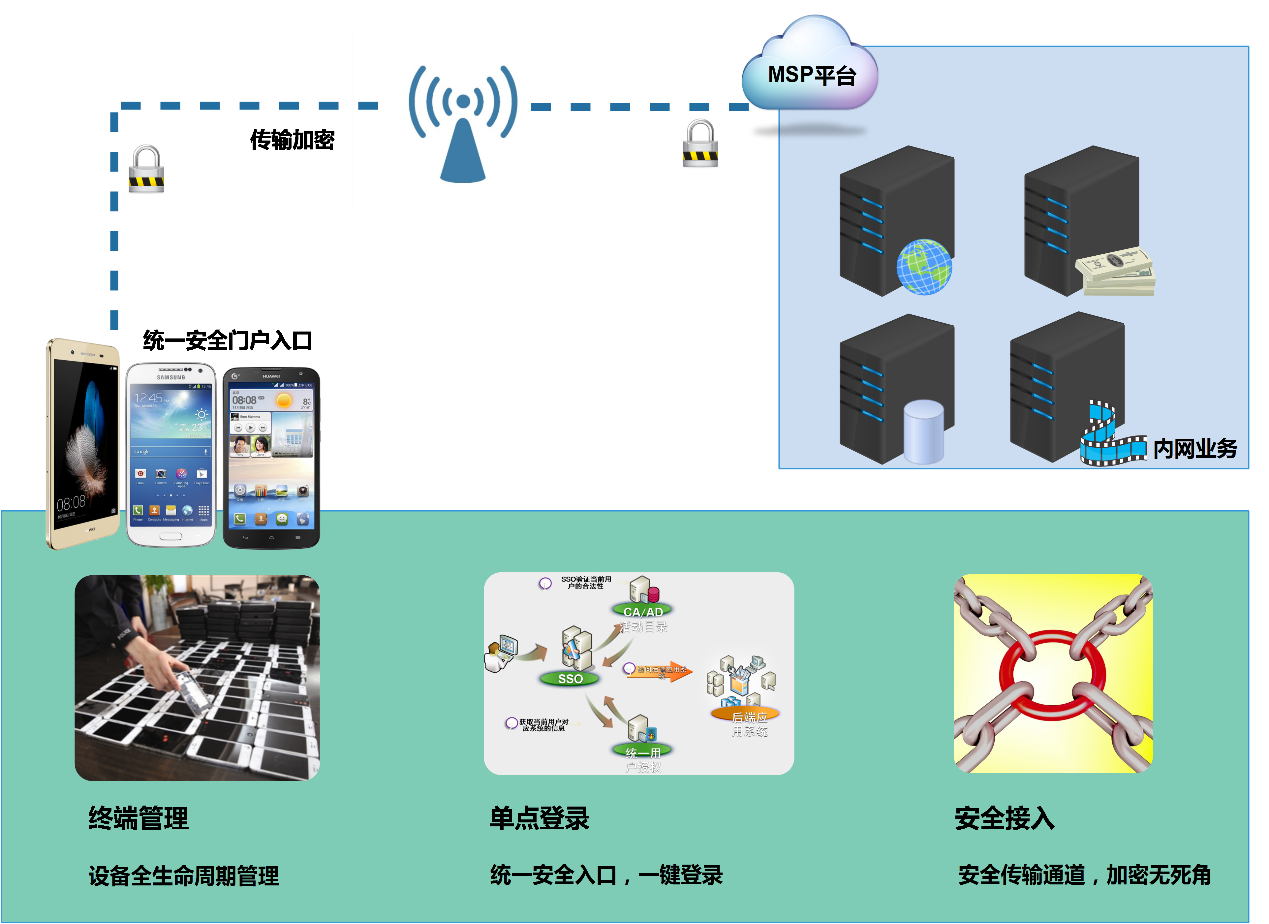
医院内网终端安全解决方案，主要集中在终端管理、数据隔离安全加密，移动查房、护理应用安全锁定，终端远程协助等主要点上。

如下图所示：



## 政府方案(1)

政府私有云终端管理平台，打造统一的终端安全门户，一键登录，多业务使用的单点系统，终端全生命周期管理、数据加密、传输加密，集安全和简单为一体的综合解决方案。



## 政府方案（2）

**无纸化会议方案**

**安全隔离：**会议文件安全隔离，高强度加密

**封闭安全空间：**内置专用文档、视频阅读器，防复制、粘贴。保证文档只有安全工作区才能使用

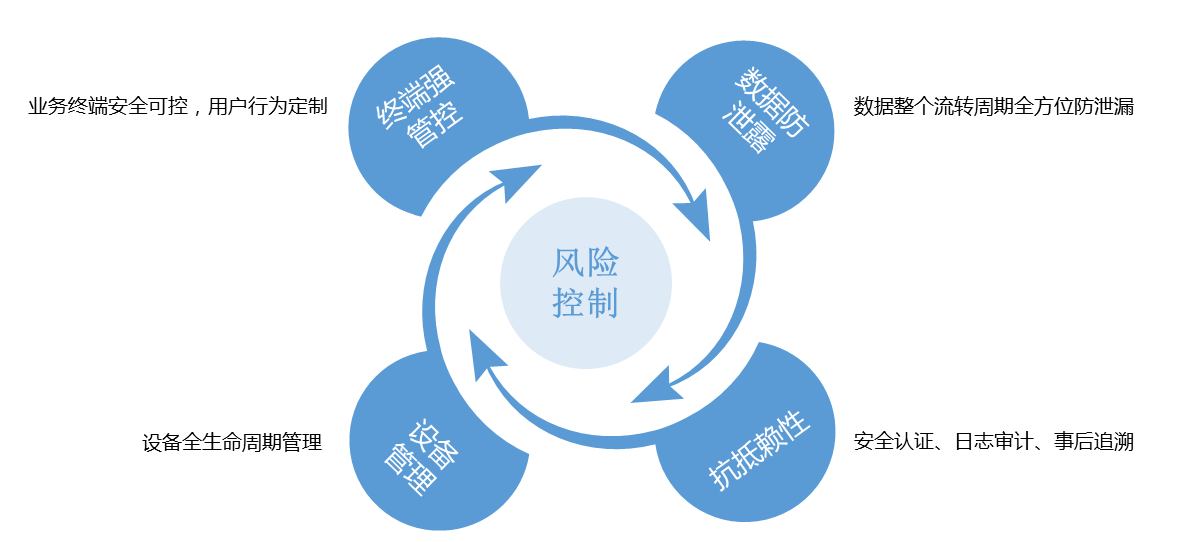
**分级管理：**分级管理，可创建多个会议管理员，负责文档准备、上传、分配。

**装机专用：**配合终端内置证书，实现一人一设备，专机专用。



## 金融方案

**移动金融业务安全有保障**



方案价值

**终端强管控：**一个完全为用户定制的安全桌面，桌面应用、桌面背景、桌面快捷方式根据需要设定、一个受管控的桌面，桌面锁定、应用锁定、防退出等机制根据管控需求设定，是迄今业内最全面的移动安全桌面解决方案。

**移动数据防泄漏：**全方位保证移动业务数据，提供数据的存储、传输、使用、清除整个生命周期的全防护。

**不可抵赖性：**通过客户端安全认证、GPS定位、自动水印、日志审计、泄漏追踪等多种技术手段增强业务操作不可抵赖性。

**设备全生命周期管理：**设备的获取、部署、运行、回收四个环节实现设备的全生命周期管理。

**移动金融办公安全高效**



方案价值

**打造移动安全入口：**打造一个用户需要的安全工作区，不仅提供工作所需的应用、文件资料、通讯、浏览等功能，而且为员工提供身份认证、合规准入、数据加密、安全隔离等全方位的安全保护服务。

**彻底实现公私隔离：**全球首创移动虚拟隔离技术，真正实现了应用零更改、数据真隔离的应用级沙箱。是一个不需要集成SDK或wrapping的隔离方案，可快速实现移动化落地。

**构建闭环安全空间：**封闭式的工作环境，集成文档阅读器、视频播放器、安全通讯、安全浏览器、安全相机等应用套件，实现了专区专用，让员工安全、高效的移动办公。

# 客户价值

通过集成启迪EONS企业移动安全管理平台，企业可以实现对移动信息化的安全防护，保障企业移动信息化的稳步推进，具体可以体现为以下三点：

1. 对于企业IT部门，可以提供全面的移动信息化安全解决方案。
2. 对于企业员工，可以全面保护员工隐私，提升企业员工的移动办公体验
3. 对于企业管理者，可以全面提升员工移动办公的效率，从而提升企业的经营和管理效率。



官方网站 官网微信

|  |
| --- |
| ◆ 联系信息 |
| 公司名称：北京启迪思创科技有限公司  服务电话：010-56380875 网址：http://www.qidsc.com  传真电话：010-56380810 邮箱：marketing@qidsc.com |

|  |
| --- |
| ◆ 版权声明 |
| © 版权所有2012-2016启迪思创。本文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，版权与解释权均属启迪思创所有，受到有关产权及版权法保护。任何个人、机构未经启迪思创的书面授权许可，不得以任何方式复制或引用本文件的任何片断。 |