深信服企业移动管理（EMM）解决方案

方案简介

企业移动管理 EMM（Enterprise mobile management）是指通过移动信息化管理手段，针对企业移动信息化建设过程中涉及到的企业移动设备、应用、信息等内容提供信息化管理的解决方案与服务。

深信服企业移动管理解决方案，是一种为企业用户打造的移动管理解决方案。用户通过简单的操作对智能终端进行注册，同时配置深信服 EMM 管理网关即可为用户提供移动设备管理（MDM）、移动用户管理（MUM）、移动应用管理（MAM）、移动内容管理（MCM）四项子管理方案，可以为用户提供从用户、设备到应用、内容的全面管理。

深信服移动设备管理（MDM），帮助用户批量管理移动办公设备

MDM 移动设备管理解决方案支持对移动设备进行管理，包括设备注册、设备擦除、用户关联、策略关联、状态监测等功能，帮助管理员管理轻松管理海量设备，降低运维成本。

深信服移动用户管理（MUM），帮助用户轻松管理企业用户权限分配

MUM 移动用户管理解决方案支持对移动用户的全面管理，包括 16 级用户认证鉴权、用户权限与移动设备关联等功能，轻松实现多部门用户管理以及细粒度权限管控，减轻管理员运维压力。

深信服移动应用管理（MAM），帮助用户快速便捷管理移动应用

支持手动/自动方式的 APP 安全加固、企业应用商店、移动应用单点登录等功能，简化应用加固、分发和用户登陆使用过程，为用户提供更加易用的企业应用使用环境。

深信服移动内容管理（MCM），帮助用户确保企业数据不被外泄

支持对下载至移动终端的企业数据进行管理，包括控制文档分发、控制邮件分发，为用户提供企业文档安全阅读环境，避免企业数据被动泄密。

需求及挑战

单位在移动信息化建设过程中，从开始开发到系统上线的过程中，会遇到以下几类典型问题：

- **业务系统向智能终端迁移，业务风险提升**

业务系统向智能终端迁移后，不但内部用户可以访问得到，外部用户也可以访问，如果有不法分子对服务器发起攻击，轻则导致服务瘫痪业务中断，重则导致企业数据泄密。

由于移动流量资费较贵，移动办公用户在进行办公时大多会选择通过 WIFI 网络接入办公系统，以节省流量费用。但是数据在传输和存储过程中都将以明文状态存在，一旦有不法分子蓄意对数据进行截取，将给企业带来严重的危害。

- **从传统终端迁移到移动智能终端，大批量移动智能终端难以管理**

目前主流的移动办公方式分两种：统一采购终端和用户 BYOD。但是无论是选择哪一个方案都会存在问题，就是管理员需要管理海量的移动智能终端。例如，部分用户喜欢将自己的智能终端进行 Root、越狱操作，增加终端使用的便利性，但是这种行为可以导致非法应用获取超级管理员权限,给企业带来数据泄露风险。

- **“影子 IT”盛行，严重威胁企业数据安全**

用户在用自己的设备进行移动办公时，经常会访问自己设备上的公有云应用以实现文件跨平台共享，这种情况被称为“影子 IT”。影子 IT 的存在，破坏了企业 IT 的治理环境。公有云应用的未受控使用，会导致企业机密数据分散，可能给企业造成灾难性风险。很多上市公司已经发生过多次类似事件，有的甚至导致股价重挫。

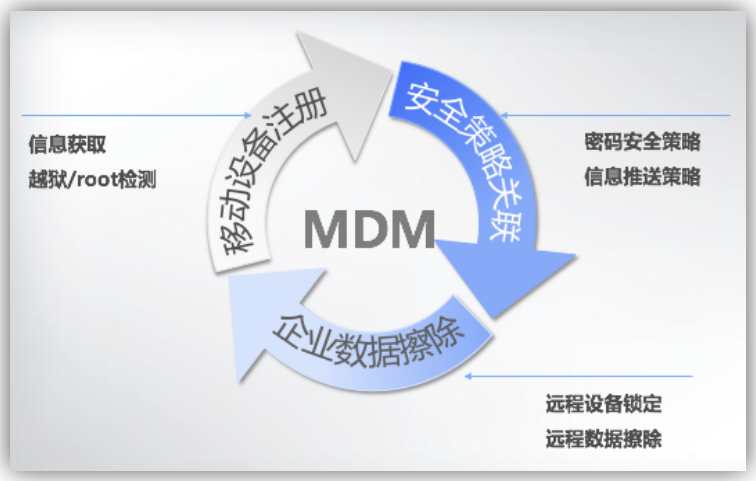
- **员工离职/移动设备丢失事件频发，机密数据泄露风险巨大**

企业办公系统移动化后，用户无可避免的需要将企业数据下载到终端上查阅使用。这样，用户就会将企业数据带出管控范围。一旦出现员工离职或办公设备丢失的情况，企业数据就容易被他人翻查，企业数据也能被其他人从手机端直接导出，造成企业应用数据泄露。

深信服的解决之道

为解决企业用户移动办公的后顾之忧，深信服发布 Sangfor EMM 企业移动管理解决方案，致力于为用户打造安全、可控、易管理的企业移动办公环境。深信服在 EMM 企业移动管理解决方案中，为用户提供包括设备、人员、应用和内容四个维度，全面的移动管理解决方案。

- **移动设备管理（MDM），轻松管理大批量企业移动办公设备**



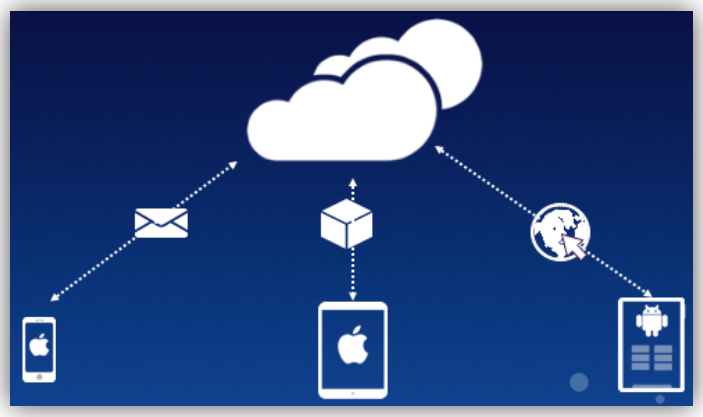
深信服企业移动管理的移动设备管理（MDM）方案可轻松使贵单位具备批量设备管理能力。当移动办公用户使用移动办公系统时，系统会按照用户权限策略要求，提示用户进行设备注册。用户注册后，管理员即可对该设备进行基础信息查看及相应的策略管控。可查看的信息包括用户设备名称、关联用户、注册时间、设备型号、操作系统、手机串号、是否 Root/越狱、设备状态是否正常等，一旦设备出现违规情况，系统界面会对管理员发出消息通知，管理员可根据以上信息对违规设备进行消息推送、设备锁定、数据擦除、弱口令拒绝等操作，强制用户终端达到公司规定的安全级别，以此保证数据不外泄。

- **移动用户管理（MUM），用户鉴权更准确，资源划分更清晰**

MUM 方案可为企业应用新增用户认证方法，包括用户名/密码、硬件特征、短信、动态令牌、CA 证书、LDAP/Radius 单点登录等认证方式，可以对企业移动办公用户的用户身份进行高强度识别，避免用户名/密码被非法人员窃取后，冒用被盗用户身份信息登录办公系统、导致信息泄密的情况出现。

同时，MUM 方案可为移动办公接入系统新增资源权限划分功能，可以拒绝企业移动办公用户访问未经授权的业务系统，避免黑客对单位内部其他系统肆意发起跳板攻击。用户在进行身份鉴权后，单位管理员可为不同部门划分不同的系统访问权限，用户仅能访问权限允许范围内的系统，为系统移动化迁移的安全性加多一层保障。

- **移动应用管理（MAM），快速加固移动办公 APP**



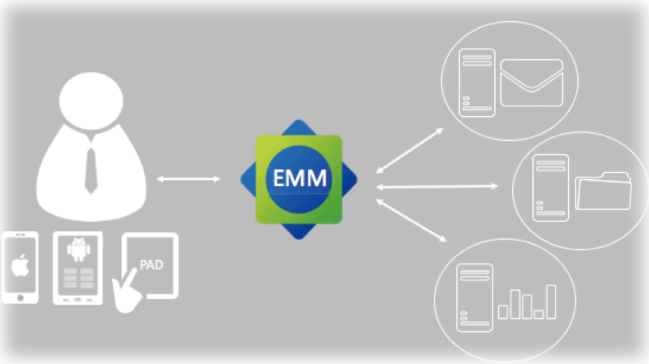
深信服移动应用管理（MAM）支持对移动办公 APP 进行安全加固，深信服可为 PC 应用提供安全加固 SDK 用于手动封装，对 Android、IOS 智能终端应用提供手动/自动两种形式的安全加固 SDK 封装。完成应用封装以后，数据在存储和传输过程中都处于被加密和隔离的状态，保障业务系统的安全性。

- **企业自建应用商店，一键发布移动办公 APP**

深信服移动应用管理（MAM）方案支持为用户自建企业应用商店。完成安全加固后的企业应用可在管理平台上一键发布给接入用户，为企业应用提供一个权威的应用分发门户。用户可以通过客户端或网页形式访问企业应用商店下载、安装，规避将企业应用分发至公共用户商店后被盗版、篡改带来的风险。

- **应用图形锁，安全、快速的 APP 重复认证**

深信服移动应用管理（MAM）方案还支持为企业应用新增应用图形锁功能，原本的企业应用从后台切换至前台时，都被要求重新认证，以保证数据的安全性。具备该功能后，重新认证方式被替换为输入图形解锁码，这样及防止企业应用未退出、其他人使用该用户手机偷窥机密信息的情况出现，又能简化用户重复认证登录过程，极大的平衡了企业应用的安全性和易用性。同时，该功能可以与 MDM 进行策略联动，锁定多次解锁失败的设备，防止图形码被暴力破解。



- **移动应用单点登录，安全前提下最佳用户体验**

深信服 MAM 方案预留可扩展的移动应用单点登录模块，在移动办公系统逐渐增多、各个系统间用户名/密码不同的情况下，为用户提供企业应用一键单点登录的功能，免除用户反复多次输入繁琐的

用户名密码的麻烦，提高用户对单位 IT 部门的满意度。

- **移动内容管理（MCM），帮助用户确保企业数据不被外泄**

深信服移动内容管理（MCM）方案支持与移动设备管理模块进行联动，根据用户终端的不同状态，对终端进行不同的应用策略管理、应用数据远程擦除甚至设备恢复初始化等操作。全面保障企业的业务系统安全。

深信服移动内容管理（MCM）方案还能够隔离个人数据及企业应用数据，如果员工离职，可以将企业应用数据擦除，避免企业敏感数据泄露的风险。如果设备丢失，还能够擦除终端所有的个人数据和企业应用数据，防止信息泄露给个人和企业带来的风险及危害。