



深信服企业移动管理EMM

为企业提供移动化管理一站式的解决方案

sangfor、SINFOR、深信服、 为深信服公司已注册或已申请的商标

深圳市南山区学苑大道1001号南山智园A1栋
市场咨询热线：400-806-6868 服务热线：400-630-6430
邮编：518055 邮箱：market@sangfor.com.cn



关注深信服官方微信
了解最新动态



EMM
免费申请试用



打造高效的企业移动管理平台

- 一站式智能管理
- 全方位安全体系
- 卓越的用户体验



移动信息化：企业发展必然趋势

移动信息化带来企业安全和管理新挑战

- 25%** 2017年 1/4的企业将建设完成自己的企业应用程序商店
- 50%** 2017年全球超过50%的企业员工会采用BYOD的方式办公
- 80%** 2015年国内EMM市场规模较2014年将增长80%
- 85%** 85%的企业不愿意将企业私有移动应用发布到公共应用商店
- 85%** 2020年全球85%的企业将全部采用BYOD办公
- 250亿** 2015年国内企业级移动信息化市场规模大约在250亿左右

01 业务系统向智能终端迁移，业务面临风险提升

业务系统向智能终端迁移后，内部服务器对外暴露，不法分子针对服务器发起攻击，导致服务器瘫痪业务中断，甚至引起企业数据泄密。同时，当移动办公用户通过Wi-Fi网络接入办公系统时，数据在传输和存储过程中都以明文状态存在，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。

02 员工离职/移动设备丢失事件频发，数据泄露风险大

企业办公系统移动化后，企业数据不受管控范围的限制。一旦出现员工离职或办公设备丢失的情况，企业数据易被他人翻查，同时也能被他人从手机端直接导出，造成企业应用数据泄露。

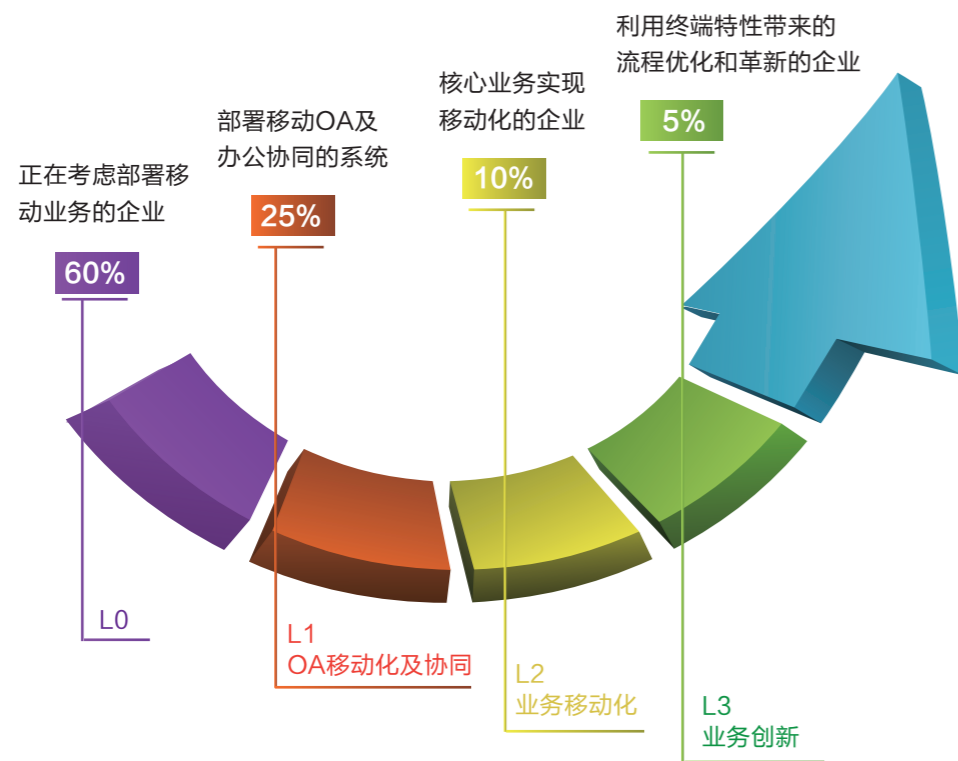
03 各种私人应用泛滥，带来效率和安全双重危险

企业给员工统一配发智能终端，但员工却安装游戏、QQ等个人应用，严重影响办公效率。同时移动办公时，用户经常会访问设备上的公有云应用以实现文件跨平台共享，公有云应用的未受控使用，导致企业机密数据分散。

04 从传统终端迁移到移动智能终端，带来管理和运维难题

企业采用移动终端进行办公的同时，也就给IT管理人员带来了海量的管理和运维工作：大规模移动设备的管控，用户认证和权限的划分，成千上万个移动应用的分发与策略授权，使运维工作量成指数上升。

企业从传统办公向智能终端迁移需经历OA移动化及协同、业务移动化和业务创新三个阶段。



数据来源：深信服2015年亚太巡展万人调研报告



深信服企业移动管理EMM

为企业提供移动化管理一站式的解决方案

1 方案概述

深信服企业移动管理（Enterprise Mobility Management, EMM）致力于为用户打造安全、可控、易管理的企业移动办公环境。员工只需要下载一个EMM套件，简单登录、注册后，IT管理员即可从移动设备管理（MDM）、移动用户管理（MUM）、移动应用管理（MAM）、移动内容管理（MCM）四个维度，有效解决移动业务开展过程中遇到的各种安全风险难题，并提升移动终端、APP应用的管理效率。



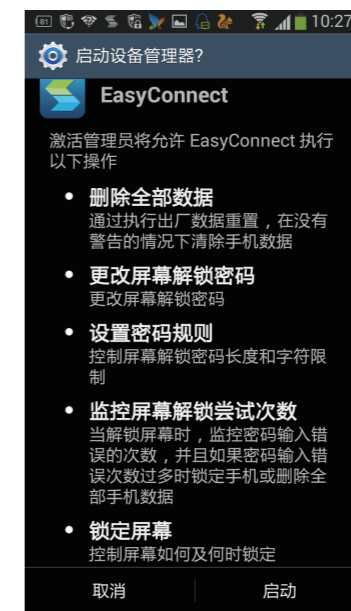
2 方案组成

01 移动设备管理（MDM），轻松管理大批量企业移动办公设备

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，帮助管理员轻松管理海量设备，降低运维成本。



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。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。



EMM设备注册



管理员消息推送

设备名称	关联用户	设备型号	操作系统	注册时间	状态
android-5w00	test	MX2	4.3.3	2019-10-01 00:00:00	失联 违规 设备已擦除
android-5w00	test	MX2	4.3.2	2018-10-02 00:00:00	失联 违规 设备已擦除
android-6569565	test	Galaxy S2	4.1	2019-10-08 00:00:00	失联 违规 设备擦除中
iOS 7.2	test	iPhone 4	7.3	2019-10-01 00:00:00	失联 违规 设备擦除中
android-510	zqm_test	MX2	4.2.3	2019-10-08 00:00:00	失联 违规
android-508400	test	MX2	4.3.1	2019-10-01 00:00:00	失联 违规
小米手机1	test	MX2	4.3.2	2019-10-15 00:00:00	失联 设备已擦除
android-5w01	test	MX2	4.3.4	2018-10-02 00:00:00	失联 设备已擦除
iOS 7.2	test	iPhone 4	7.1	2019-10-01 00:00:00	失联 设备擦除中
iPhone of Mike	test	iPhone 5S	7.04	2018-10-02 00:00:00	失联 设备擦除中
android-5r0	test	MX2	4.0.3	2018-10-01 00:00:00	失联
iPhone-9	test	iPhone 4	7.0.1	2018-10-02 00:00:00	失联
iPhone-5"	extra	iPhone 4	7.1.1	2019-10-01 00:00:00	违规 设备已擦除
iPhone-7"	zqm_test	iPhone 4	7.1.0	2019-10-01 00:00:00	违规 设备已擦除
iPhone-3	test	iPhone 4	7.2	2019-10-01 00:00:00	违规 设备擦除中
小米手机A1	test	MX2	4.3	2019-10-01 00:00:00	违规 设备擦除中
IPHONE-E	extra	iPhone 4	7.1.1	2019-10-01 00:00:00	违规
iPhone-8	test	iPhone 4	7.2.1	2019-10-01 00:00:00	违规

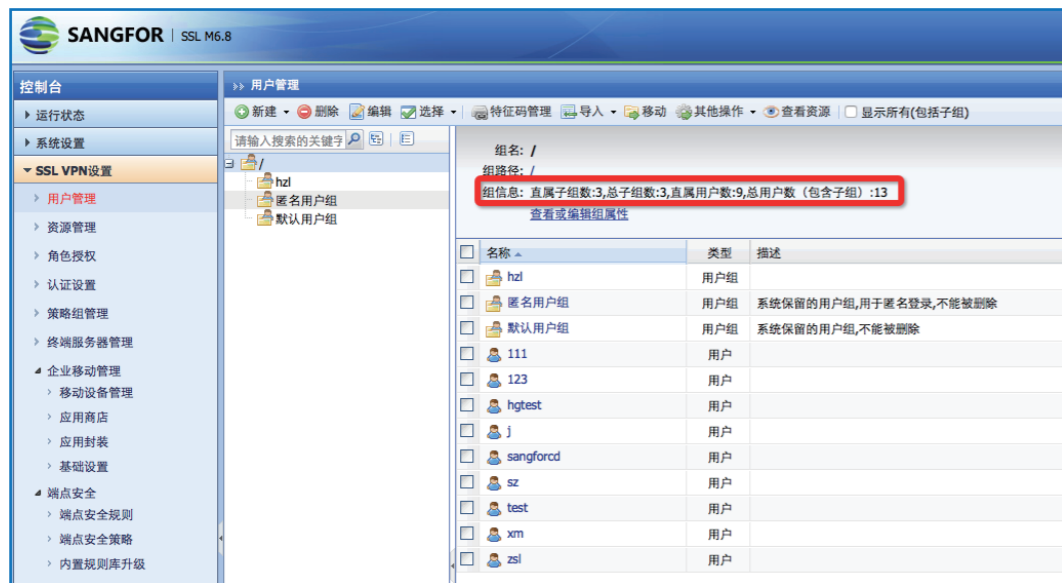
用户与设备关联

02 移动用户管理（MUM），用户鉴权更准确，资源划分更清晰

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、7种认证方式、用户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。



移动用户登录认证



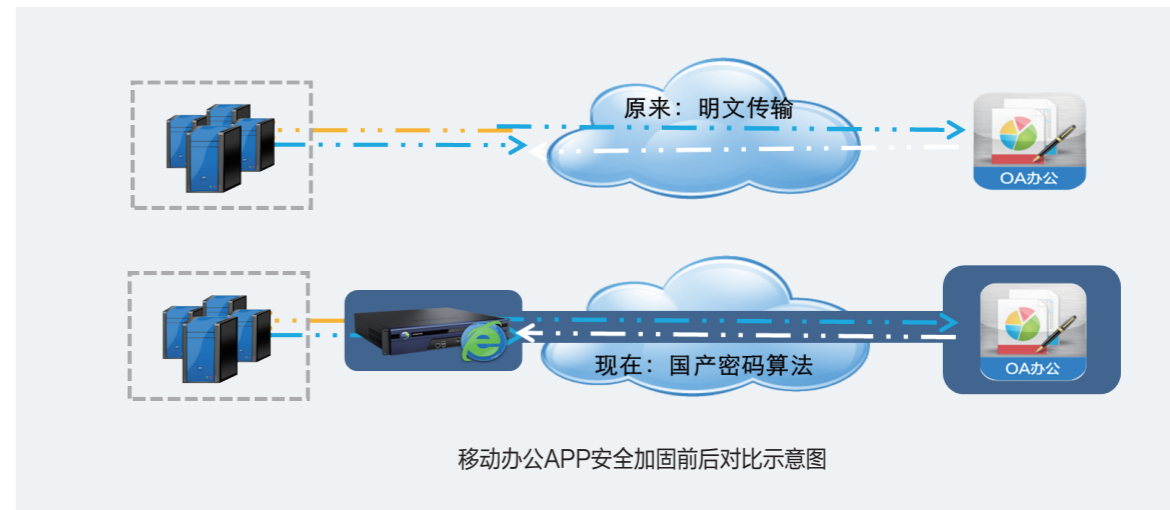
多级组织架构

03 移动应用管理（MAM），企业应用更安全，运维管理更便捷

MAM移动应用管理方案支持手动/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。

● 应用封装，快速加固移动办公APP

移动应用管理MAM支持对移动办公APP进行安全加固，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，企业数据与个人数据将被逻辑隔离。

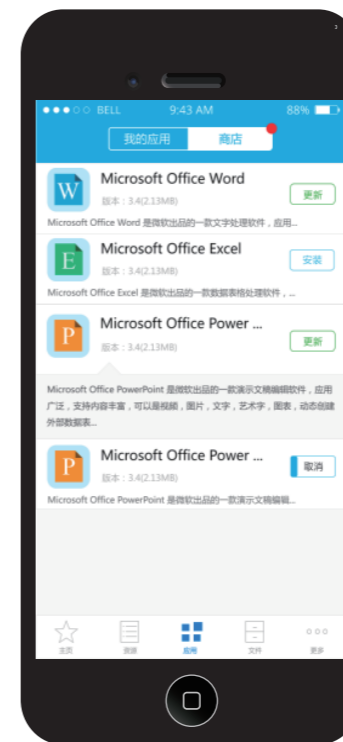


移动办公APP安全加固前后对比示意图

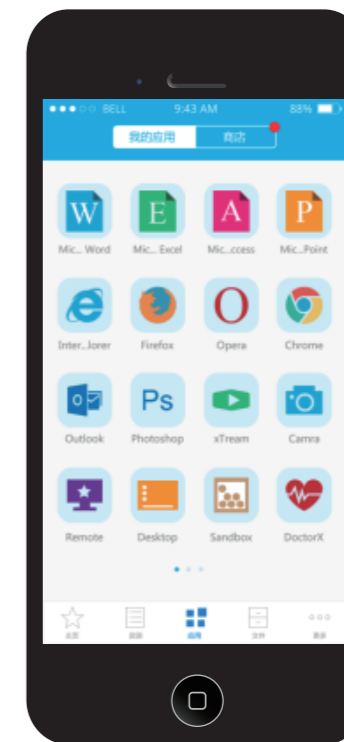
● 企业自建应用商店，一键发布移动办公APP

移动应用管理MAM支持为用户自建企业应用商店。企业应用完成安全加固后，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。

同时，移动应用管理MAM支持对应用分发时进行策略授权，如：仅允许应用在手机或平板上安装，限制该应用的使用用户等。既可满足应用分发需求，又能控制企业应用不被非单位用户下载使用，一举两得。



应用按权限分发到商店



用户下载并安装

应用名称	适应平台	版本	文件大小	分发范围	下载次数	发布时间	状态
移动营销	Android(手机、平板)	1.6	28.18 MB	所有用户	0	2013-05-13 10:39:04	正常
电子政务系统	Android(手机、平板)	1.0	5.32 MB	所有用户	0	2013-05-05 12:13:54	正常
移动协同	Android(手机、平板)	2.3.0	5.23 MB	所有用户	0	2013-04-16 12:25:58	正常
移动协同	Android(手机、平板)	5.1.3	10.81 MB	hzi	0	2013-03-28 09:20:07	正常
移动协同-手机-成都办	Android(手机、平板)	5.1.3	17.47 MB	默认用户组	0	2013-03-03 08:55:13	正常
曝工资	Android(手机、平板)	5.7.50303	4.41 MB	hzi	0	2013-02-26 14:05:03	正常
Ping_and_DNS	Android(手机、平板)	2.0.6	2.66 MB	hzi	0	2013-02-24 18:44:12	正常
飞常准	Android(手机、平板)	3.0.2	9.21 MB	xm	0	2013-02-23 19:00:35	已下架
网信通-联通版	Android(手机、平板)	3.3.3	12.61 MB	所有用户	0	2013-02-23 12:16:29	正常
移动协同HD	IOS(iPhone、iPad)	5.1.7	14.06 MB	所有用户	0	2013-02-20 09:33:24	正常

应用商店管理界面：适用平台、下载统计、状态查询

● 应用黑白名单：应用权限有效管控

目前很多企业统一分发智能终端进行移动办公，移动应用管理MAM可对这些智能终端进行应用的管控，例如现在在工作时间只能使用移动办公系统，不能进行QQ聊天、淘宝购物、刷微博等娱乐活动，提升员工办公效率。



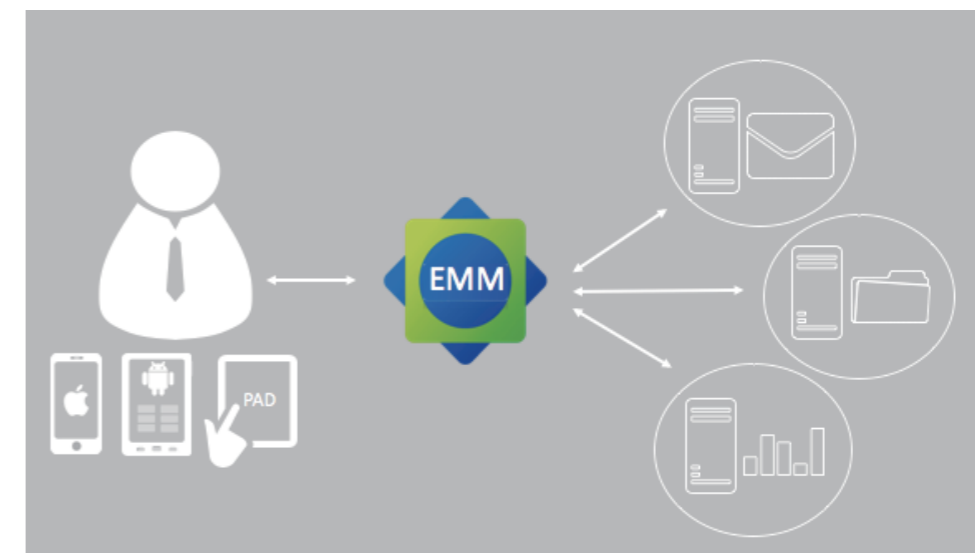
启用应用黑名单后，运行QQ提示该应用被禁用

应用名称	应用ID	版本	大小	数据大小	应用类型	是否违规
ES文件浏览器	com.estrongs.android...	3.2.5.2	11 M	468 KB	普通应用	正常
EasyConnect	com.sangfor.vpn.clien...	6.9.4.3.24265	25 M	42 M	普通应用	正常
Easyapp	com.sangfor.easyapp	1.0	15 M	61 KB	普通应用	正常
Firefox	org.mozilla.firefox	37.0.2	33 M	4 M	普通应用	正常
L3VPN	com.sangfor.l3vpn	1.0	15 M	317 KB	普通应用	正常
QQ	com.tencent.mobileqq	5.6.1	34 M	23 M	普通应用	违规
UC浏览器	com.UCMobile	10.4.0	45 M	0 KB	普通应用	正常
UIMonitor	com.sangfor.vpn.uim...	1.0	1 M	25 KB	普通应用	正常
tclient	com.t.tclient	1.0	1 M	0 KB	普通应用	正常
去哪儿旅行	com.Qunar	7.3.8	27 M	0 KB	普通应用	正常
微博	com.sina.weibo	4.5.0	41 M	0 KB	普通应用	正常
手机淘宝	com.taobao.taobao	4.2.0	24 M	0 KB	普通应用	正常
手机百度	com.baidu.searchbox	6.5	43 M	540 KB	普通应用	正常

控制台界面出现违规告警

● 移动应用单点登录，安全前提下最佳用户体验

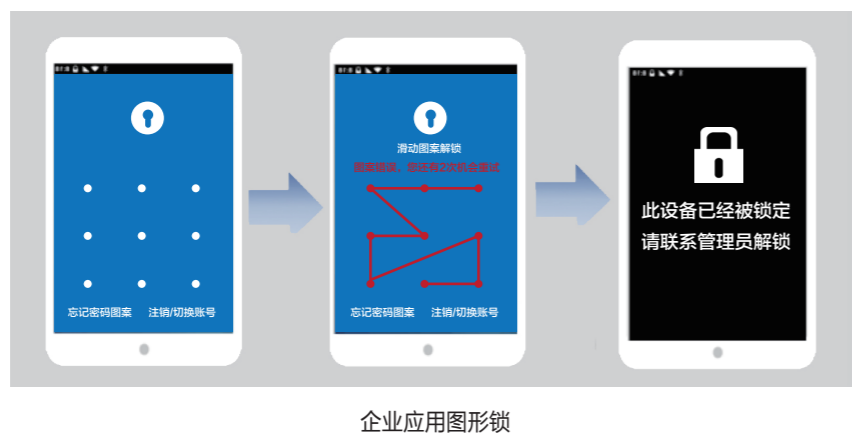
移动应用管理MAM预留可扩展的移动应用单点登录模块，在移动办公系统逐渐增多的情况下，为用户提供企业应用一键单点登录的功能，免除用户反复多次输入繁琐的用户名密码的麻烦，提高用户的满意度。



单点登录功能示意图

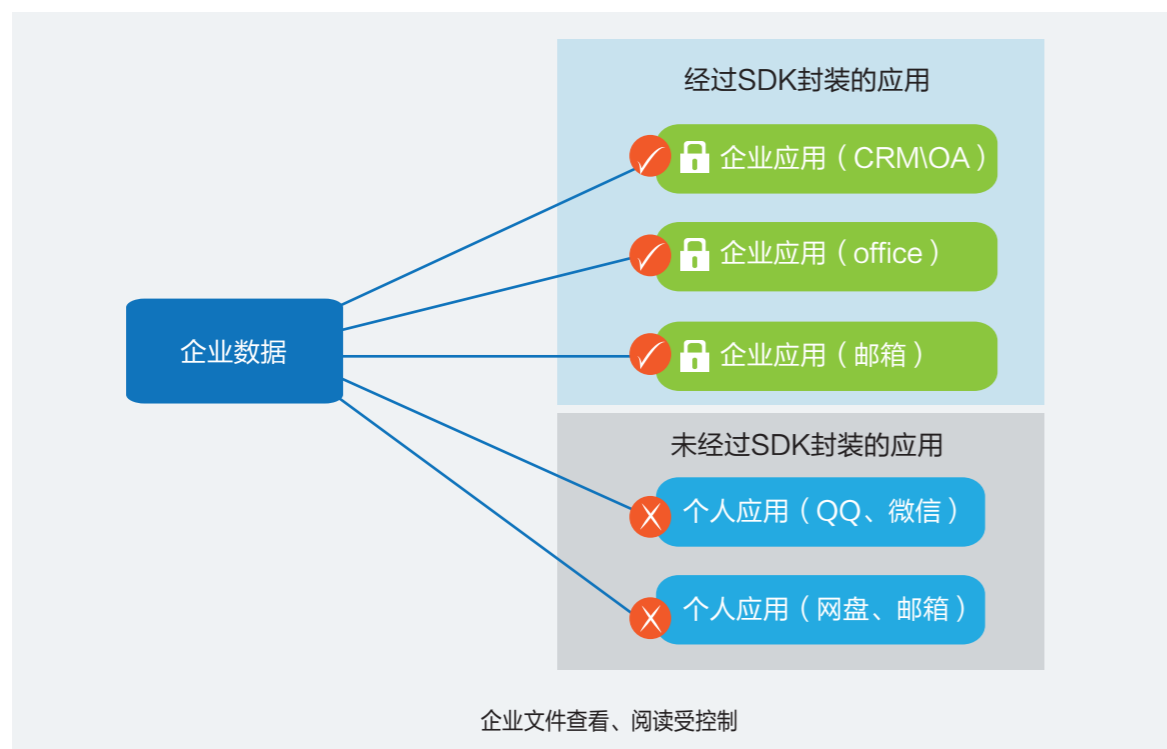
● 应用图形锁，安全、快速的APP重复认证

移动应用管理MAM支持为企业应用新增图形锁功能，企业应用从后台切换至前台时，只需要输入图形解锁码，即可完成重新认证，既能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。

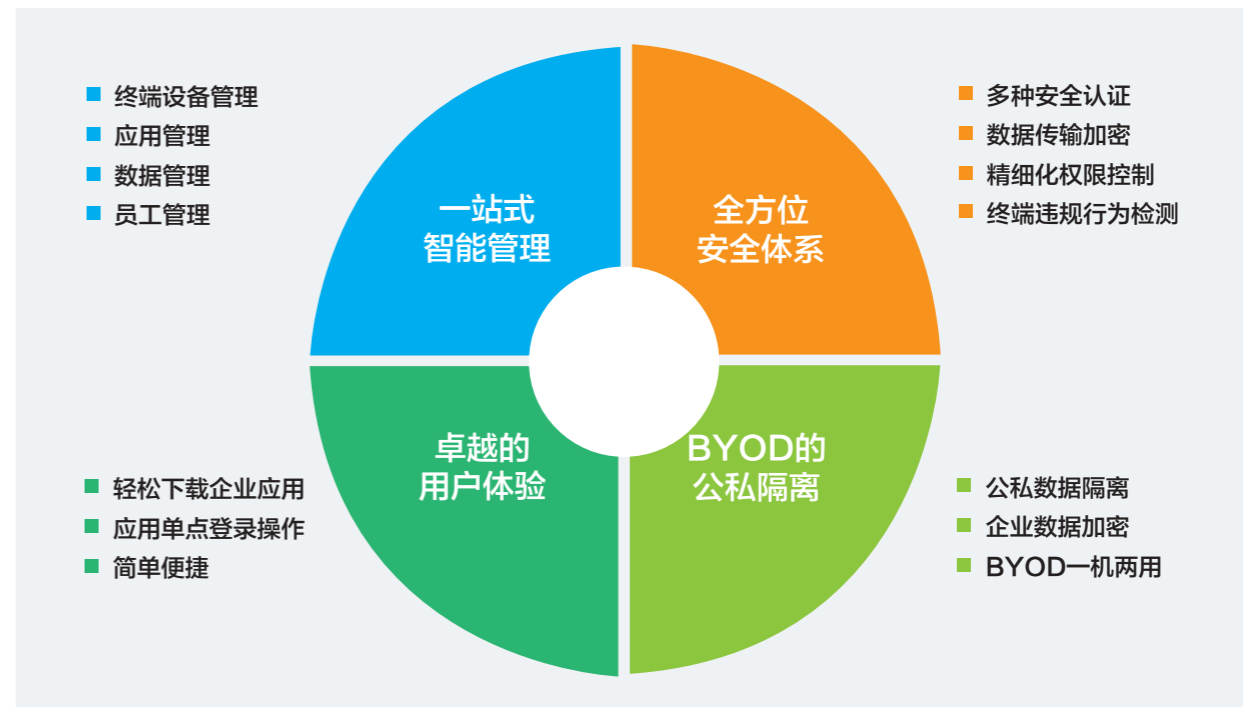


04 移动内容管理（MCM），帮助用户确保企业数据不被外泄

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或设备恢复初始化操作。同时该方案支持对下载至移动终端的企业数据进行加密，加密后的文件仅能在经过安全加固后的企业应用中打开，即使文件被上传至百度网盘等应用中，也无法打开。



深信服EMM方案特点与优势



EMM行业应用场景

