深信服 EMM 技术白皮书

深信服科技股份有限公司

2017 年 XX 月 XX 日

目录

1.企业移动化趋势与挑战

1.1. 企业移动化趋势

1999 年黑莓推出了 Push Mail 移动邮件办公，受到了企业的极大欢迎，因为邮件的移动化，能够有效的提升企业的效率。2007 年之后智能手机的普及，移动化更进一步，移动化从邮件延伸到了 OA、营销、统一通信等基础协作类应用。随着移动互联网和智能手机的发展进步，移动办公进入了优化阶段，从最开始的基础办公协作、基础业务协作，到核心业务创新。

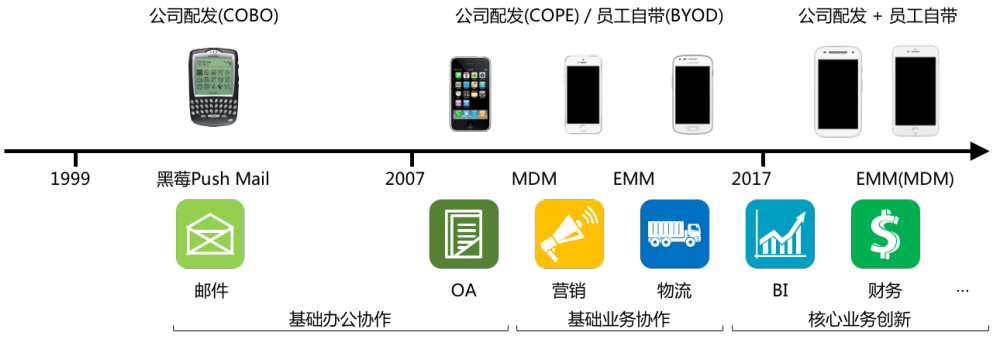


图 1 企业移动化阶段与趋势

据咨询机构 IDC 统计，企业在 2017-2018 年的规划向核心业务的移动化延伸，例如 CRM、ERP、自动销售系统、BI 系统等；另外，部分企业还处在基础业务协作阶段，投资建设 IM、会议、协同、企业社交等应用。在此同时，移动安全的建设投入最大，可见企业认为安全问题是企业移动化的前提。

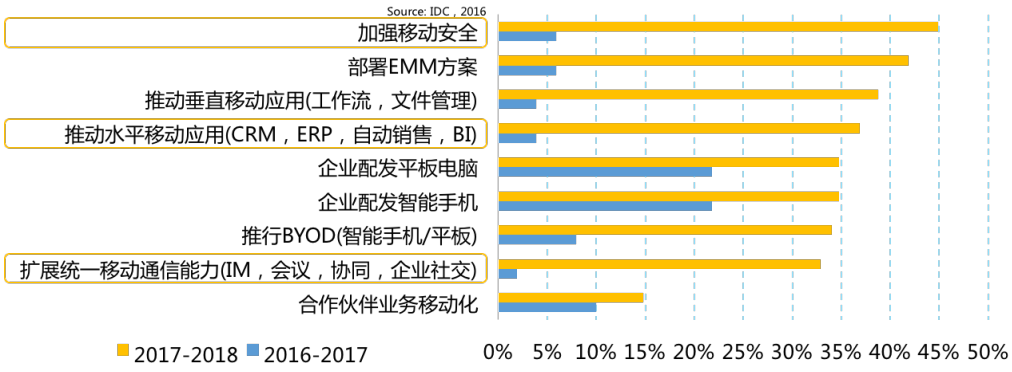


图 2 企业移动化建设规划统计

1.2. 企业移动化安全与实施挑战

企业业务移动化时，要考虑诸多泄密风险，如设备丢失，USB 拷贝，微信 QQ 分享，明文传输被监听， 中间人攻击，入侵窃取服务器机密文件等等，防不胜防。可以说，数据泄密问题是移动办公建设的拦路虎。

移动化之后，企业核心数据存储在员工手机上，难管控。据调查，60% 的员工会在离职时有意识的收集 并带走公司资料；另外，手机容易丢失，也会导致设备上的敏感信息泄露。保护移动数据，挑战巨大。

企业的移动业务数据在不安全的 Internet 上传输，如果网络数据没有进行高安全级别的加密保护，那么数 据很容易被黑客监听，甚至是被篡改，最终会导致无法估计的损失。

移动 App 的应用服务器部署在公网，应用服务器的 IP 信息暴露，将使得恶意黑客通过扫描手段探测服务器， 发现可用的操作系统、中间件、数据库、应用服务的脆弱点，进而采用攻击和入侵手段，窃取敏感数据。

移动办公设备型号多，版本高低不齐，实施安全管控时，兼容性问题突显，导致部署和运营效率低下；另外， 安全管控会降低移动应用体验，致使员工使用率低。兼容性和易用性差，是业务移动化实施和推行的绊脚石。

移动办公的特点是设备多版本杂，采用传统的安全封装方式，如 ROOT 提权保护，技术复杂，难实施； 如集成安全 SDK，需要额外的适配开发测试，影响业务迭代上线更新。如果没有一个兼容性好的方案， 安全封装实施挑战巨大。

通过自建下载页面来管理企业应用，应用下载权限无控制，发布上线慢，手工链接下载费时费力；无应用 更新实时推送，在线应用版本多，导致维护工作量大，投诉增多。如果应用分发不畅，会严重影响移动业 务全员推广覆盖。

很多增加了安全管控的应用，额外的认证操作多、应用响应速度变慢，与个人应用体验差异巨大；员工满 意度低，导致移动应用使用率低，移动业务推行缓慢。

2.企业移动管理(EMM)产品价值

EMM 平台提供各种安全和移动 App 集成特性，将企业 IT 基础设施与移动网络和移动终端集成，将企业 IT 应用延伸到移动设备上，用以提升企业业务效率、提高员工工作满意度、降低企业成本。

2.1. 保护企业数据安全

EMM 平台产品支持端到端的移动安全方案，保护企业 IT 数据在移动业务流中存储、传输的安全，降低因数据泄露而对业务造成的经济、法律、品牌等方面的风险。

2.2. 移动化提升企业业务效率

EMM 可以减少企业 IT 和动化安全保护实施门槛，通过高兼容性和易用性设计，支持企业员工主流的智能手机，免开发支持移动业务 App 的安全封装，并且提供一站式的移动应用商店服务，加速企业移动业务 App 上线之后的全员覆盖。

EMM 在提供安全保护的同时，提供企业 App 高用户体验，不改变企业员工的移动应用使用习惯，保证企业员工的满意度，提升企业应用的使用率，真正的落地企业业务移动化，最终提升企业业务的效率，并为企业未来利用移动化进行业务创新打下基础。

3.深信服 EMM 产品概述

3.1. 深信服 EMM 产品定位

深信服 EMM 解决方案定位于政府、金融、大企业等各个行业的移动业务安全保护，包括移动数据在终端存储、网络传输、后台服务器上的安全；同时，深信服

提供完整、便捷的移动安全应用加固解决方案，一站式的移动应用商店，并且保证封装后的移动应用的体验与个人应用一致。

3.2. EMM 总体架构

图 3 深信服 EMM 总体架构图

深信服 EMM 方案架构上包含移动终端、统一认证与安全接入、自动化封装服务、企业应用商店、移动设备管控五个逻辑组件，其中自动化封装服务、企业应用商店、移动设备管理合称为移动数据安全管理平台。移动数据安全管理平台与企业应用服务器和认证服务器对接，完成移动 App 与企业 IT 基础设施的集成。

3.3. 深信服 EMM 方案简介

深信服 EMM 包含 EMM-EasyApp、EMM-EasyWork、EMM-EasyWork+三个子方案，满足不同客户不同移动化阶段的需求。

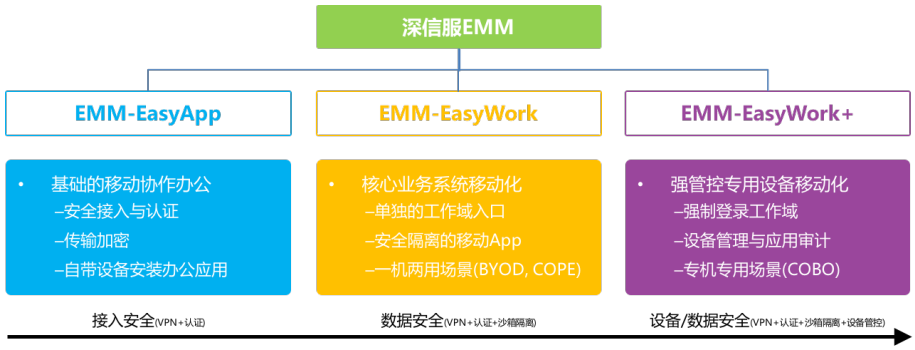


图 4 深信服 EMM 三大子方案

3.3.1. EMM-EasyApp

EasyApp 支持移动办公应用 VPN 安全接入。移动 App 通过轻量级 SDK 集成或自动封装，快速支持 VPN 接入，保护数据传输安全；移动应用服务器部署在内网，系统信息和漏洞被隐藏，有效降低恶意攻击和入侵的安全风险。加固后的安全应用可以安装在员工手机上(BYOD)和企业配发设备上(COPE)，快速满足移动邮件、移动 OA 等基本的移动办公需求。

3.3.2. EMM-EasyWork

EasyWork 支持安全工作域数据安全。提供统一的移动工作域，内置安全邮件客户端、安全相册等基础应用，企业可通过自动封装加固，快速新增安全应用，如移动 CRM、移动 ERP 等。安全应用完全与个人域隔离，防止 USB 拷贝、社交共享、剪切板、截屏等手段泄密，满足企业使用员工设备(BYOD)或企业配发设备(COPE)进行核心业务移动化需求。

3.3.3. EMM-EasyWork+

EasyWork+支持移动数据安全与设备严管控制。设备开机强制进入安全工作域，用户只能使用工作域中的应用，如移动展业、移动营销等应用，防止使用个人应用影响效率。在应用安全隔离的基础上，对外设和网络连接进行严格控制，并支持多种安全合规审计，更进一步降低数据泄密风险，满足企业使用配发设备(COBO)进行强管控的核心业务移动化需求。

4.深信服 EMM 产品功能

4.1. 移动应用安全接入

深信服 EMM 方案采用 SSL VPN 接入方案，支持 3 层 VPN 和 4 层 VPN 接入。3 层 VPN 支持承载多个移动 App 的数据加密传输，4 层 VPN 支持一个移动 App 的数据加密传输。

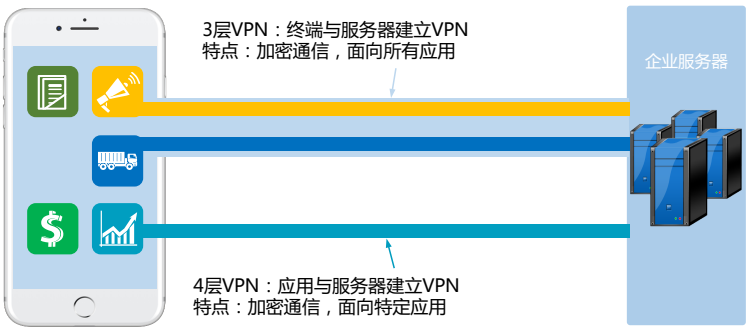


图 5 深信服 EMM 移动 VPN 接入技术

4.1.1. SSL 传输加密

深信服 EMM 方案中的移动应用采用安全的 SSL 加密协议，保证移动 App 在传输中的安全。SSL 协议具备良好的安全性和网络穿透性，广泛适用于各个行业的安全传输加密。

深信服是 SSL VPN 市场的领导者，采用标准的 SSL 加密协议。

握手协议：客户和服务器之间相互鉴别 -协商加密算法和密钥 -它提供连接安全性，有三个特点 身份鉴别，至少对一方实现鉴别，也可以是双向鉴别 协商得到的共享密钥是安全的，中间人不能够知道 协商过程是可靠的。

记录协议：SSL 记录协议建立在可靠的传输协议（如 TCP）之上 它提供连接安全性，有两个特点 保密性，使用了对称加密算法 完整性，使用 HMAC 算法 用来封装高层的协议。

警告协议：这个协议用于每时示在什么时候发生了错误或两个主机之间的会话在什么时候终止 。

SSL 协议数据交互的过程如下：

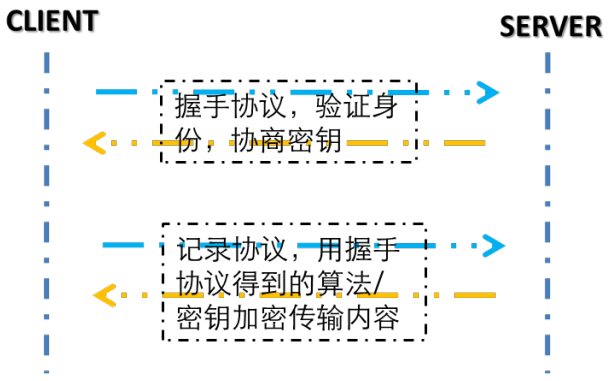


图 6 SSL 协议标准

4.2. 移动安全工作域

深信服 EMM 向企业员工提供移动应用安全工作域，是移动应用的统一入口，所有的移动应用均可以快捷的访问，减少员工需要区分个人应用和工作应用造成的不便，提升应用体验。

4.2.1. 办公应用统一入口与一机两用

深信服 EMM 办公应用统一入口和沙箱隔离，完美支持一机两用模式，企业数据在个人设备上被完全隔离，能够防止个人设备病毒木马的恶意攻击，以及员工的有意无意泄密。员工离职或者设备丢失之后，可以远程擦除设备上的企业数据，保证企业的数据安全。

同时，企业应用不会对个人的应用造成影响，完全保护员工个人应用的隐私，使得员工工作和生活两不误。

4.2.2. 强制工作域与专机专用

对于企业的核心生产系统，企业会配置专用的移动设备来支撑业务，这些设备仅能用作业务，不能用于个人用途，例如微信/QQ 聊天，或者存储个人文件或照片等。这种专用设备必须被企业有效管理，保证设备本身和设备上企业数据的安全。

深信服 EMM 的 EasyWork+子方案支持 Android 设备专机专用场景，设备启动之后强制进入安全工作域，员工无法使用访问到个人应用，在工作域中只能安装和使用企业管理员配置的移动应用。

同时，专用设备可以被企业管理员进行全生命周期的设备管理，包括 Android 系统的基础功能管控、数据通道管控、应用使用管控等等。

深信服专机专用方案支持终端免定制，并支持完整的数据安全和设备管控、审计能力、移动应用商店能力等。

4.3. 完善的认证准入功能

深信服 EMM 平台支持多种身份认证方式，例如本地认证、LDAP/AD 认证、CA 认证、硬件特征码认证、手势认证等，满足客户不同的认证需求。

4.3.1. 本地数据库认证

深信服 EMM 内置本地认证数据库，支持客户自助创建用户组和用户账号、密码，不同的用户组支持不同的移动应用下载权限和应用服务器访问权限。

4.3.2. Radius 认证

如企业已经采用 Radius 进行用户的认证管理，可进行 EMM 平台与 Radius 的联动。在 EMM 平台中建立相应的用户组结构，并勾选 Radius 认证并绑定相应的 Class 属性值。用户向 EMM 平台提交提交用户名密码认证信息时，EMM 平台将此信息以标准的 Radius 协议格式向 Radius 服务器发起认证请求，Radius 将返回认证结果。若 Radius 认证通过，则将在返回给 EMM 平台的数据包中捎带 Class 分组属性，EMM 平台将根据绑定该属性的用户组赋予该用户相应的认证、策略、授权等属性。若 Radius 认证未通过，EMM 平台则将拒绝该用户登录。

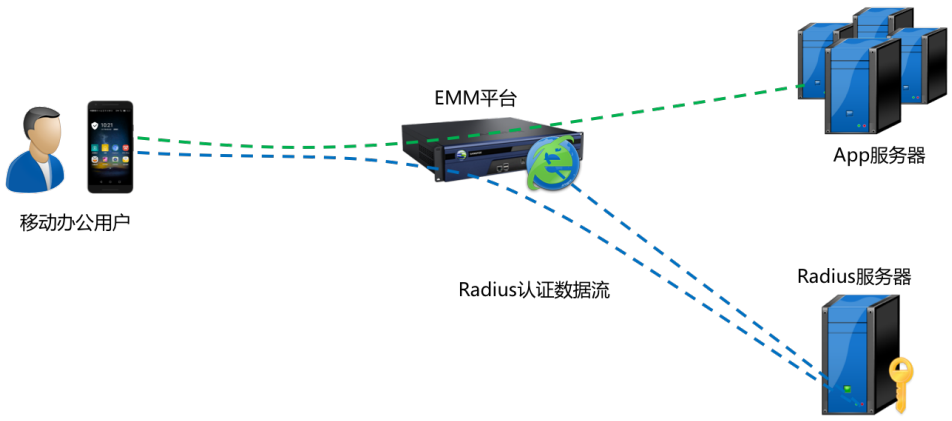


图 7 EMM 平台 Radius 用户认证

4.3.3. LDAP 认证

如企业已经采用 LDAP 进行用户的管理，EMM 平台可与 LDAP 进行联动，只需在 EMM 平台中根据 LDAP 中的 OU 组结构建立用户组结构，并为用户组绑定相应的 OU 结构，无需再设备中一个个建立具体用户。当用户向 EMM 平台提交用户

名密码进行身份认证时，EMM 平台自动将此认证信息提交给 LDAP 进行认证，并根据反馈信息判断该用户是否为合法用户。当用户通过了 LDAP 认证，EMM 平台将根据 LDAP 返回该用户的 OU 值，将该用户自动归于绑定了该 OU 的用户组，该用户即享用该用户组所有认证、策略、授权等属性。

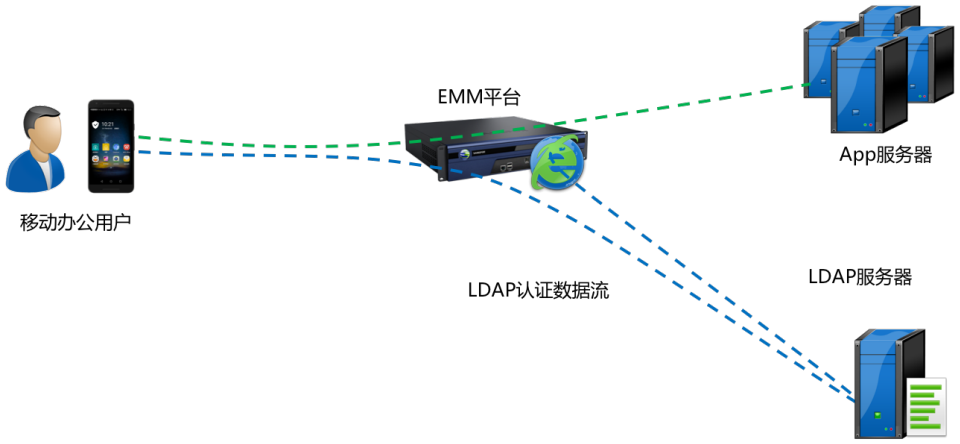


图 8 EMM 平台 LDAP 认证

4.3.4. CA 认证

EMM 平台内置了 CA 中心，完美支持 PKI 体系。通过 EMM 平台内置 CA 中心，企业或者事业单位可自建 CA，避免单独购买 CA 的额外投资，减少投入成本。同时，EMM 平台也可无缝支持已有的第三方 CA 认证。

图 9 EMM CA 管理

在数字证书使用的过程中必然涉及到数字证书的过期等问题，为了更好的保持与证书状态信息的同步，EMM 平台支持 OCSP 服务器，实时保持与 OCSP 服务器的同步，让所有证书的状态信息都能够及时得到反馈，保证 CA 证书认证的安全性。

图 10 EMM CA 证书同步

4.3.5. 硬件特征码认证

对于仅使用用户名/密码认证的用户，为了保证 EMM 用户登录限定在某一台或是某几台终端上，因用户帐号意外泄漏、帐号盗用导致数据的泄露问题，可对登录终端进行绑定。

通常的终端绑定都是采用 IP、MAC、IP/MAC 绑定的方式实现，但是对于 EMM 用户，采用这样的终端访问方式是不合适的。移动用户需要走出局域网远程访问，IP 地址经常是不固定的。而标识网卡的 MAC 地址也能进行手工的改动，导致终端存在被仿冒的威胁。

深信服 EMM 打破常规，通过终端的硬件特征码绑定实现硬件终端的唯一标识。通过获取客户端的不可改变的硬件信息，如 CPU、存储、网卡等信息生成数字证书，并对证书和用户进行绑定实现用户身份的唯一性控制。

当用户登录 EMM，客户端的控件就会自动获取终端的硬件信息生成一串数字与字母结合的 HardID 并传送到 EMM 平台设备。需要进行绑定的账号用户工作平台若是在不同的客户端上，我们可按不同用户、用户组实际需要设置不同的特征码的个数（1-100 个硬件特征码），保证终端绑定安全的基础上实现人性化的管理。

图 11 EMM 硬件特征码认证管理

4.3.6. 手势密码认证

深信服 EMM 支持移动的手势解锁认证，当应用超过 1 分钟无操作后，用户再次使用的时候，需要输入预设好的手势密码，一方面防止打开的应用应用被偷窥、被旁人操作造成的信息安全风险，另一方面手势认证简化了解锁操作，减少了输入解锁密码的步骤。

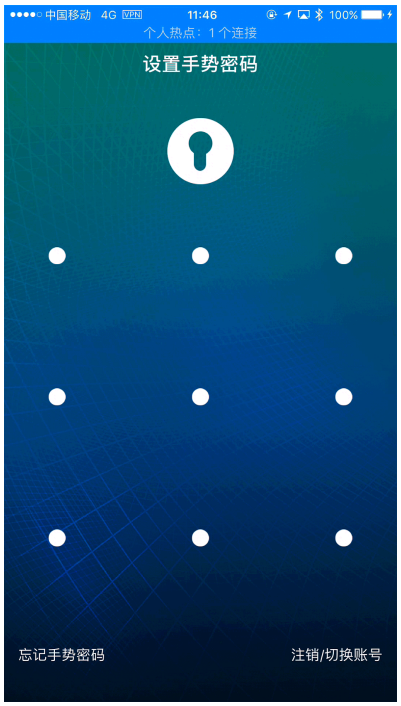


图 12 EMM 客户端手势密码认证

4.4. 便捷的移动应用单点登录

4.4.1. 移动应用单点登录录制

深信服 EMM 支持企业移动 App 的单点登录，避免二次登录带来的体验性问题，员工不必记忆多个企业 App 的账号和密码。

深信服 EMM 单点登录采用录制的方式实现，管理员在应用封装后，获取移动应用的登录界面，生成自动登录代码封装到移动应用中。

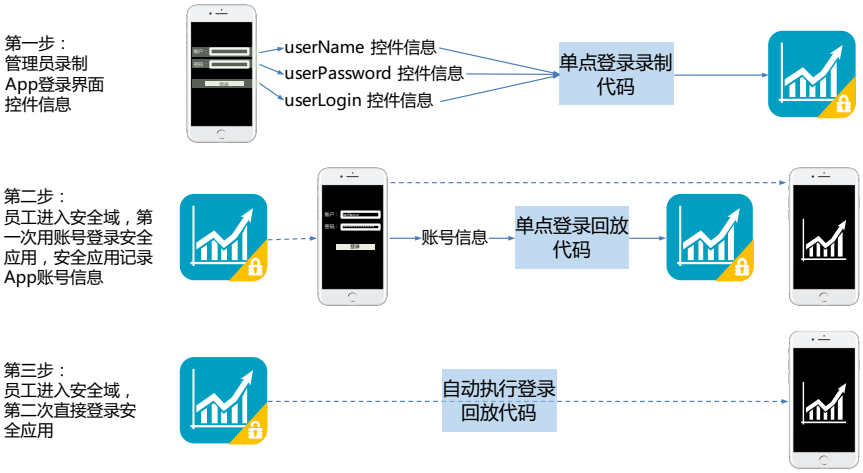


图 13 企业应用单点登录

4.4.2. 应用单点登录

员工第一次登录时输入账号信息，后续打开应用时，应用会自动执行登录过程，从而实现单点登录。

4.5. 移动安全隔离技术

深信服 EMM 采用创新的沙箱隔离技术，将工作域中的应用与个人域完全隔离，包括剪切板、文件系统、文件分享、网络传输等等，有效的防止个人域病毒木马攻击的同时，阻止员工恶意泄密的行为，保护企业的敏感数据的安全。

图 14 EMM 客户端安全隔离

4.5.1. 文件加密隔离技术

深信服 EMM 创建了一个完整的虚拟文件系统，这个文件系统只能被工作域中的 App 和服务访问。工作域中的 App 访问文件系统时，会调用工作域中的文件 API，之后工作域文件系统会调用个人域操作系统的文件系统，写入数据后进行强加密，或者解密后读取文件信息。

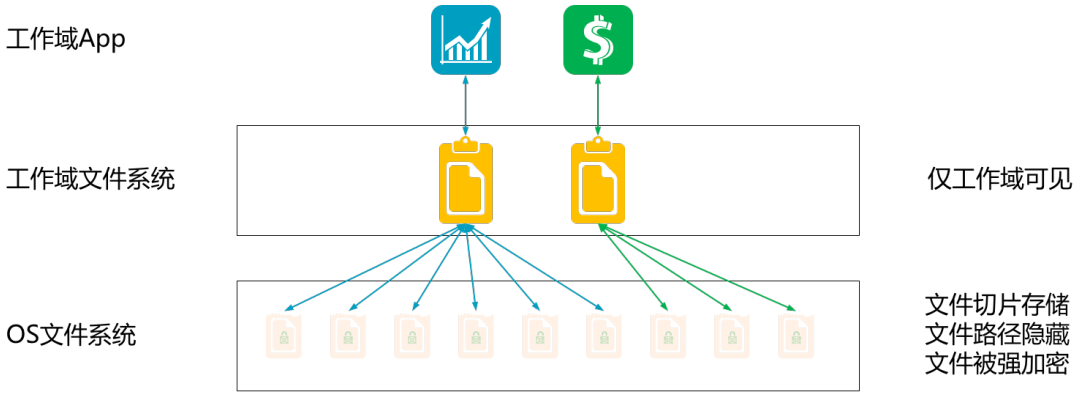


图 15 文件加密隔离

安全域文件在操作系统中存储时，采用分片存储的方式，而且文件路径对个人用户隐藏，即使黑客获取了分片文件，也很难合并成完整的文件，而且文件经过了高强度加密，进一步保证了文件的安全性。

4.5.2. 剪切板隔离技术

深信服 EMM 安全域的剪切板与个人域也是隔离的，在企业移动 App 中拷贝的数据只能拷贝到其他企业移动 App 中，无法拷贝到个人域的应用中，防止员工将敏感信息有意或者无意泄露到互联网中，造成企业不可控的损失。

4.5.3. 文件分享隔离技术

在移动社交网络发达的今天，在移动设备上进行文件信息分享非常方便，已经形成一种习惯。但是文件分享会对企业信息造成安全威胁，因此深信服 EMM 方案提供移动应用分享隔离的方案。企业 App 中的文件只能在安全工作域内进行分享，而无法分享到微信、QQ、百度云盘等互联网应用中去。

4.5.4. 防截屏技术

员工使用手机截屏功能能够获取移动办公应用的敏感信息，因此深信服 EMM 方案提供企业应用防截屏的功能，防止员工截取企业敏感信息进行泄密。

4.6. 应用安全封装

管理员在 EMM 后台上传 APK、IPA 文件之后，填写应用信息，选择需要封装的安全特性，即可提交 EMM 平台封装。

图 16 EMM 设备管控方案

4.6.1. 支持 iOS/Android 主流版本

图 17 移动应用上传 EMM 平台

深信服 EMM 采用系统底层技术进行安全代码的自动封装，支持 iOS 和 Android 的主流版本，兼容性具备天然的优势，覆盖员工使用的移动设备的各种机型和各种版本，避免因为版本不兼容造成的 IT 运维成本。应用封装之前，管理员获取 Android 或者 iOS 企业应用，上传到 EMM 平台。

4.6.2. 安全策略封装

深信服 EMM 方案支持双域隔离应用的安全封装，封装之后，企业 App 具备安全隔离的功能，使得企业 App 快速获得移动应用数据安全的能力，包括剪切板隔离、分享隔离、文件隔离等。如图 18 配置安全策略所示。

图 18 配置安全策略

4.7. 应用商店管理

深信服 EMM 方案支持一站式的企业应用商店服务，移动应用进行安全封装之后，即可通过应用商店后台进行统一的发布，员工即可在 EMM 客户端中应用商店进行应用的下载或者更新。

图 19 EMM 应用商店

4.7.1. 应用发布

企业应用进行安全封装之后，即可发布到企业应用商店中，发布过程简单易用。在应用发布时，支持应用的版本号管理，方便应用商店提醒用户进行应用的更新。

4.7.2. 应用权限管理

深信服 EMM 应用商店支持应用下载的权限管理，不同的部门和角色员工具备不同的应用下载权限。通过细致的应用下载权限的管理，防止非工作需要的员工越权访问移动应用和数据造成的数据安全泄密风险。

4.7.3. 应用推送

应用发布之后，EMM 方案支持实时推送新应用信息，使得员工可以及时获取、安装新的应用，方便移动业务快速全员的覆盖。对于已有应用，版本更新之后，通过应用实时更新推送，员工快速更新应用，减少因为移动应用版本不齐带来的运维成本。在 WiFi 环境下，移动应用更新文件可自动下载，员工只需要确认即可快速安装。

4.7.4. 应用列表统计

EMM 应用商店提供全面的信息统计功能，方便企业管理员了解所有在应用商店发布的移动应用，每个应用使用的移动平台，版本号信息，应用的分发角色，以及应用下载安装的设备数量。所有这些信息均可以文件导出，方便统计分析。

应用名称	适应平台	版本	分发范围	安装设备数/设备总数	下载次数
口袋助理	IOS(iPhone、iPad)	2.5.3	所有用户	0/32	16
DingTalk	IOS(iPhone、iPad)	3.3.1	所有用户	0/32	3
Chrome	IOS(iPhone、iPad)	36.1985.57	北京办	0/11	2
QQ浏览器	Android(手机、平板)	7.4.0.3130	jiang,五粮液,…	2/9	8
口袋助理	Android(手机、平板)	2.5.3	所有用户	0/19	8
WPS Office(…	Android(手机、平板)	9.6.1	所有用户	4/19	13
安全相机相册…	Android(手机、平板)	1.0	所有用户	4/19	11
安全浏览器(…	Android(手机、平板)	Developer	所有用户	5/19	11
安全邮箱(公…	Android(手机、平板)	1.0	所有用户	2/19	10
wlyoa	Android(手机、平板)	6.0.17	五粮液	0/2	1
微信	Android(手机、平板)	6.5.7	demo,大连办,宁…	0/12	4
QQ	Android(手机、平板)	6.7.1	demo,五粮液,崔…	0/9	5
wpsoffice	IOS(iPhone、iPad)	7.0.0	所有用户	0/32	19
QQ邮箱	IOS(iPhone、iPad)	5.2.1	所有用户	0/32	25

图 20 应用商店统计报表

4.8. 移动设备管理

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。

图 21 EMM 设备管控方案

4.8.1. 便捷的批量移动终端管理

移动设备管理方案可轻松使 IT 部门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，贵单位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。

4.8.2. 严格的设备密码策略

移动设备管理方案可以强制用户必须将密码设置为带有字母和数字的复杂密码；可强制手机超时自动锁屏；可设置修改密码规则（新密码与旧密码不能一样）；可设置密码有效周期，例如 1 个月要重新设置一次密码；可防止暴力破解，在多次输入错误密码时删除所有数据。

4.8.3. 远程锁定移动设备

通过设备管理方案的设备锁定功能，管理员可以远程锁定手机，让违规手机无法使用。Android 设备被锁定之后，设备将无法正常使用，目前只能从控制台进行解锁；iOS 设备被锁定之后，设备上输入解锁密码即可继续使用。

4.8.4. 远程擦除办公终端数据

手机丢失、人员离职等情况下，把手机还原到出厂状态，擦除终端上的所有数据，避免企业信息泄露。

4.8.5. 企业消息推送

设备管理方案集成消息推送功能，管理员可以定向给用户推送通知信息。有时候需要群发放假、会议等通知。为了企业数据安全，有些用户规定移动办公专用设备不允许安装 QQ、微信等应用，企业也没有内部专用的即时通讯系统，发邮件不一定经常接收，发短信成本较高。这种情况下，利用移动设备管理的消息推送功能可以将信息直接推送给所有移动办公用户，以上问题就解决了。

4.9. 应用服务器保护

将深信服 EMM 平台以单臂方式部署，通过配置使数据流经由 EMM 平台后走向内网服务器区，对办公网与服务器区这两部不同安全级别的区域进行隔离。由于 EMM 平台对外只开放 443 端口，从而可屏蔽掉其他端口的攻击。EMM 平台的数据流处理方式可隐藏内网服务器区结构，并对服务器访问的 IP、域名进行伪装。EMM 平台在进行用户对服务器区发起的访问时，采用 SSL VPN 登录认证、细粒度应用访问授权、传输数据加密，从数据安全的角度提供隔离保护。

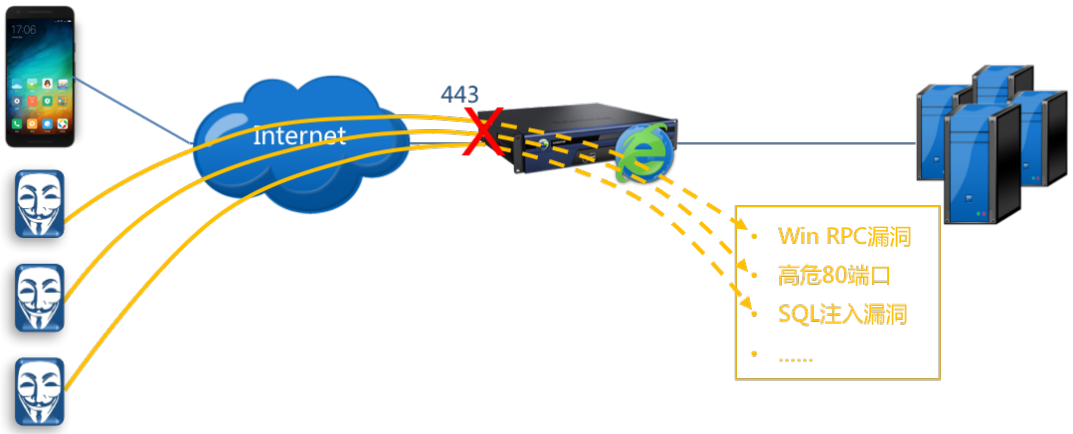


图 22 移动应用服务器隐藏

5.深信服 EMM 技术优势

5.1. 高度的数据安全性

深信服 EMM 方案，支持企业移动业务的全方位数据安全保护。统一的移动安全工作域，与个人域完全隔离，防止终端侧恶意泄密；移动应用网络接入传输全程加密，防止信息监听与篡改；移动应用服务器隐藏，数据封闭保护。

5.2. 全面的系统兼容性

深信服 EMM 不需获取 ROOT 权限即可实现应用安全加固，兼容多种系统，不需要改动代码，无额外开发人力与时间成本。天然支持 BYOD 和企业配发设备一机两用(COPE)模式，满足不同企业移动办公方式需求。

5.3. 良好的分发易用性

企业应用商店能轻松管理安全移动应用，员工可快速获取应用，并支持应用的自动推送，加速应用的分发推广；同时，App 应用商店作为唯一的下载源，轻松避免恶意篡改应用被安装，保证移动业务的安全性。

5.4. 一致的移动化体验

深信服 EMM 提供一个单独的移动工作域，所有办公 App 可以通过统一入口访问，方便快捷；移动办公应用与个人域 App 体验一致，保证了员工使用移动业务的满意度，为移动业务的推广扫清障碍。

6.深信服科技股份有限公司

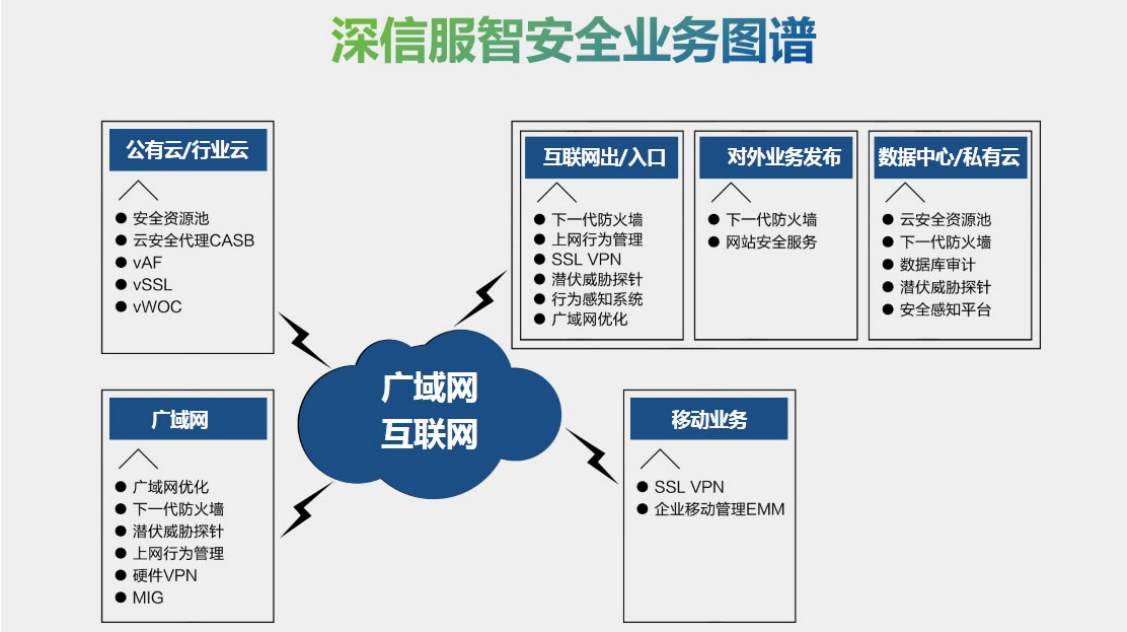
深信服科技股份有限公司成立于 2000 年，专注于安全与云计算领域，致力于让用户的 IT 更简单，更安全，更有价值。经过 17 年的发展，深信服在全球共设有 56 个直属分支机构，员工规模超过 3500 名。2016 年年销售额达到 21.6 亿元。

（一）业务概览

1、深信服智安全：专注做实用的安全，让每个组织的安全建设更有效、更简单

在安全业务上，深信服是中国企业级安全领导者。包括硬件 VPN、上网行为管理、SSL VPN 和广域网优化在内的多款安全产品取得了市场第一的成绩。下一代防火墙产品，在同“下一代防火墙＋传统防火墙”的品类竞争中，仍取得了市场占有率第三的好成绩。

基于“做实用的安全，让每个组织的安全建设更有效、更简单”的安全业务目标，深信服在广域网、移动业务、互联网出口、对外业务发布以及数据中心场景的安全需求场景下，提供了相应的安全解决方案。在公有云与行业云，以及私有云等场景下的安全需求，深信服也提供了安全资源池等解决方案。



2、深信服云 IT：用创新打造简单、稳定、安全、易用的云 IT 新架构，致力于让每个企业的 IT 更具价值创造力

在云计算业务上，深信服是成长最快的企业级云计算厂商。企业云应用案例年增长超过 800 个；超融合架构入围了 Gartner2016 年《X86 服务器虚拟化基础架构魔力象限》，包括深信服在内，国内仅有两家厂商入围；桌面云产品实现了从前端到后台的一体化交付，1000 台以上应用案例超过 100 家，累计交付终端超过 25 万台；应用交付产品连续 5 年入围 Gartner 国际魔力象限，也是连续 3 年市场第一的国产品牌。

深信服云 IT 以业务为中心，关注关键业务上云的过程，让 IT 云化更简单。为政府及企事业单位提供从数据中心、分支机构到云终端三方面完整的云计算产品、解决方案及服务。

- 企业云：基于创新的超融合架构，为用户快速构建私有云、混合云、行业云，将用户的 IT 资源池化、IT 使用服务化、IT 运维自动化，让关键业务轻松上云。
- 分支云：借助全新的软件定义广域网技术，帮助集团型企业实现对各地分支机构的 IT 集中管控、自动化部署，以及分支零运维，总部管理更敏捷。
- 桌面云：通过前后端软硬件的深度融合，只需桌面云一体机和云终端，即可实现桌面云平台的快速交付，为用户打造媲美 PC 体验、更安全、更高效的桌面云。

深信服创新的云 IT 新架构，通过提供简单、稳定、安全、易用的 IT 基础架构，让用户 IT 投资成本节省了 30%，应用上线时间缩短了 50%，运维复杂程度降低了 60%。用户的 IT 部门将释放更多精力投入业务创新，以支撑企业的规模增长。

（二）发展策略

6.1. 重视研发，深信服持续创新

一直以来，深信服都十分重视研发，持续将年收入的 20%投入到研发，并在深圳、北京、长沙和硅谷设立了四大研发中心，研发人员比例达 40%，其中 30%拥有硕博学历。在对创新发展的持续投入下，深信服获得了众多突破性创新，包括全球第一台 IPSec / SSL 二合一 VPN 网关、创造了上网行为管理品类、全球首家将网络虚拟化融入超融合架构、国内首家推出下一代防火墙、国内首家推出云安全资源池等。2016 年，深信服新增的发明专利申请达到 122 件，截至目前已经累计申请专利总数达到了 506 件。其中，“下一代应用防火墙系统及防御方法 ”获得了“中国优秀专利奖”。

深信服始终基于用户需求展开创新，并设立系列创新机制。研发人员每月例行拜访用户 3 次以上，收集用户的实际需求。每年收集到的有效需求超过万条，并将有效需求迅速转化为产品新版本；面向所有员工，深信服设立了年度创新奖。一等奖奖励 12 个月的工资，特等奖的奖金高达一百万；每月，深信服组织创新大师论坛，鼓励员工展示创新成果或者分享创新的经验。

多年来，深信服持续创新，2016 年新增 62 个产品新版本，推出了 aBOS 、安全资源池、安全感知平台等新产品和解决方案。2016 年，深信服还成为了国家地方联合工程实验室，博士后创新实践基地单位，为创新提供源源动力。

6.2. 重视服务，深信服全情投入

深信服始终重视用户服务。在深圳、长沙、吉隆坡设置了超过 200 坐席的 CTI 中心；在 56 个城市设立备品备件中心，产品出现故障能够立刻提供替换设备，保障业务顺畅运行；在 56 个直属办事处设有原厂工程师，全国共有 5686 名认证工程师，能够给用户提供快速的上门服务响应。

同时，深信服建立了快速响应的服务机制。深信服提供 7x24 小时的 400 电话咨询和远程调试的服务，通过手机短信推送等方式，让服务反馈及时到达用户，真正做到了服务可视化。通过深信服在线社区提供人工智能在线服务，24 小时在线提供咨询。并有各产品线研发技术专家在线解答，365 天无休。

6.3. 全球化战略

深信服始终着眼于全球，在美国、英国、新加坡、香港、马来西亚、泰国、印尼和阿联酋，设立了 8 个境外分支机构，并在这些年的发展中，获得了众多海外用户的广泛应用。同时，深信服 X86 服务器虚拟化、上网行为管理、应用交付、广域网优化、VPN 和下一代防火墙，这 6 款产品入围了国际权威 Gartner 全球魔力象限。此外，深信服还获得了 NSS Labs 最高等级推荐级证书， ICSA 防火墙证书，且检测技术创新获得了 Google 认可，加入全球顶级情报联盟 VirusTotal 。

目前，全球有近 50,000 家用户正在使用深信服的产品。其中包含 90%的政府部委单位，80%的全球 500 强中资企业、85%的 985、211 高校、排名前 20 名的银行单位。

2017 年，深信服邀请了两位世界冠军为深信服两大子品牌代言：两届奥运冠军、世界拳王金腰带获得者邹市明代言深信服智安全、里约奥运会羽毛球男单冠军谌龙代言深信服云 IT。两位世界冠军代言的是拼搏进取，勇于突破，实力夺冠的精神。深信服也将继续以这种精神创造更好的产品和解决方案，给用户业务带来更高的价值。

联系我们

售前咨询热线：400-806-6868

售后服务热线：400-630-6430 （中国大陆）

香港：（+852）3427 9160

英国：（+44）8455 332 371

新加坡：（+65）9189 3267

马来西亚：（+60）3 2201 0192

泰国：（+66）2 254 5884

印尼：（+62）21 5695 0789

深信服手机官网

EMM免费申请试用