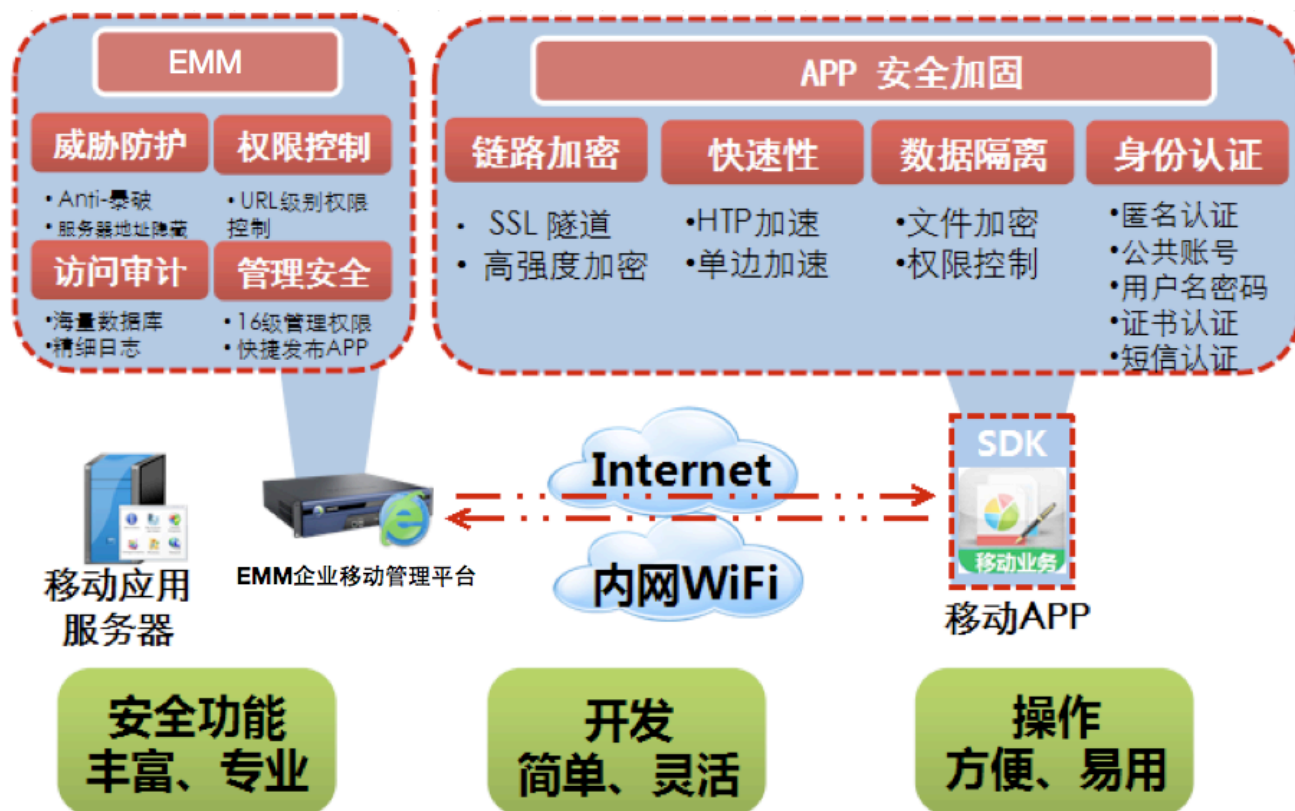


深信服应用安全加固自动封装解决方案

方案简介

深信服应用安全加固解决方案，是一种在移动应用程序中快速集成安全加密模块的方案。用户通过简单的操作对智能终端应用程序（APP）进行安全加密模块注入，配置深信服 EMM 企业移动管理网关即可实现从用户、终端、链路、服务端的全面的防护。



考虑单位移动办公数据安全的核心诉求，通过强身份认证、终端数据加密隔离、链路数据加密、权限控制与访问审计这五个维度全面的保护从终端到服务端的安全。

移动办公最主要目的是提升单位人员整体办公效率，而系统访问速度也是影响办公效率的关键因素。通过深信服自主研发的 HTP 高速传输协议及单边加速技术进行应用访问加速，无需 APP 开发人员进行单独的软件加速模块开发、也不需要移动终端用户修改任何设置，即可对移动应用完成系统加速，数据传输效率提升 15%-30%，对办公效率提升的最终目的进行二次保障。

应用背景

单位开发用以移动办公的智能终端 APP 后，员工会广泛使用，以提高工作效率。然而，办公 APP 工作过程中，办公数据由互联网未经加密直接传输会存在泄密风险。使用越频繁，安全风险越高，一旦发生非预期安全事件导致数据泄密，会危及到单位数据资产，给单位带来严重损失。系统建设者对于移动办公 APP 的安全风险应该防范于未然，通过相应的安全技术手段，来保障移动办公系统的信息安全。

需求分析

单位在开发移动办公 APP 时，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：

1、软件开发商非专业安全厂商，移动办公系统可能存在安全风险

- APP 开发厂商大多数只专攻产品功能和易用性，没有在 APP 中提供完善、成熟的安全解决方案；
- 数据明文存储、身份认证方式简单、单一，导致单位的机密数据存在被泄露的风险；
- 移动办公数据通过连入 WIFI 等网络未加密传输，极易被窃听或被拦截篡改；
- 由于软件系统加入安全模块后涉及长期的更新维护、加密算法更替等情况导致成本过高，超出预算投入范围；

2、为 APP 提供接入的服务器暴露在公网，成为安全木桶的短板

- 提供服务的 APP 服务器是通过端口映射等方式直接暴露于公网中，存在被攻击风险；
- 黑客发现、攻击服务器时，轻则导致服务器宕机业务中断，重则被黑客获取系统超级管理员权限，控制服务器、窃取和摧毁数据。

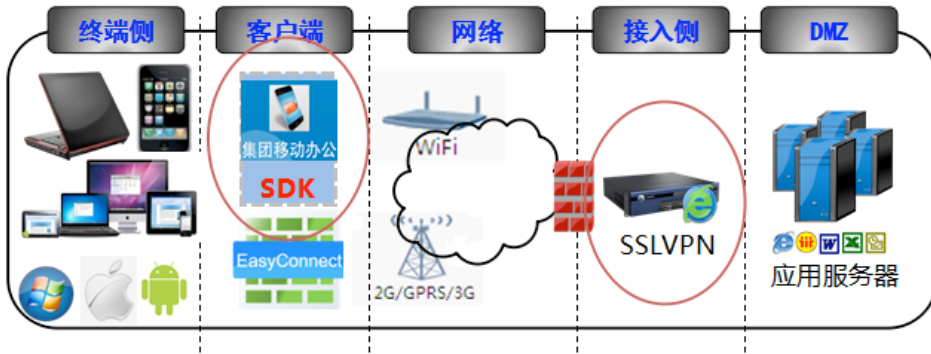
3、配置复杂、兼容性差、APP 更新迭代周期长，业务系统上线容易，用户推广使用难

- 复杂的配置、苛刻的安装维护操作大幅降低业务系统的使用效率，甚至导致用户弃用复杂的移动办公方案，使移动办公无法正常推广。

解决方案

对于单位来讲，解决以上问题，使移动办公安全、快速、易用，高效移动办公系统的建设目的才能真正达成。

为解决上述问题，深信服提出应用安全加固解决方案。深信服应用安全加固方案是一种针对企业用户利用 APP 在智能终端上开展移动业务场景下，对用户的 APP 安全接入需求提出的安全、简单、易用的解决方案。用户只需要在应用服务器接入侧部署 SSL VPN 安全网关，即可为移动办公系统提供 APP 安全加固封装平台；同时，网络只对外开放 SSL VPN 的 443 端口，将应用服务器真实地址隐藏在 SSL VPN 设备后端，断绝了黑客的攻击途径。



对移动办公 APP 完成应用封装以后，在数据存储、传输过程中都处于被加密和隔离的状态，达到企业数据与个人数据进行逻辑隔离的目的。



方案优势

深信服应用安全加固解决方案具有以下三个方面的优势：

1、安全：

- 采用集成安全代码方案，为智能终端的办公 APP 安全添加了 4 种用户认证方式，确保用户身份安全；
- 数据存储及传输过程加密，提升端到端的安全策略，全面提高单位移动办公的数据安全；
- 在公网只开放 VPN 的 443 端口，将后端服务器隐藏起来，避免暴露在公网被黑客攻击，加固业务服务器安全。

2、快速：

- 从应用没有集成安全加密模块，到 VPN 安全加密模块集成，只需要 2-5 分钟即可，并且无需研发人员配合；
- 多种加速协议优化，提高 APP 在无线网络环境下的访问速度，进一步提高工作效率。

3、易用：

- 用户只需要点击一下 APP 即可完成加密隧道建立、进行业务系统访问，无需额外的配置；
- 授权漂移机制、非对称集群技术保障业务系统平滑扩容。

典型案例

福建海事局提升政务效率，构建服务性政府

福建海事局采用 EasyConnect 和 MAM 的组合方案，通过自动封装方案“移动执法系统开发”安全性，通过现场查询、信息录入、违法处理等功能，实现了移动执法，提高水上交通违法行为快速处置能力。

提升政务效率，构建服务型政府

移动执法APP:
办理现场查询、信息录入、违法处理
结合EasyApp，提升安全性

移动办公:
8个办公系统，9个业务系统
低成本、快速实现移动办公

福建海事局有近 20 个应用系统，有两种业务场景，分别是移动执法和移动办公，如果都开发 APP，则会需要很长的开发周期和高额的成本。针对操作频繁，体验要求高的移动执法，福建海事局开发了 APP 应用，同时采用深信服 MAM 方案提升安全性；针对移动办公的业务系统，通过 EasyConnect 来进行虚拟化发布，实现十多个系统的快速、低成本迁移。



青岛银行 提升政务效率，构建服务性政府

青岛银行开发了信用风险管理 APP，让一线客户经理，能够在客户现场更准确、更及时的获得客户信用风险信息，不但提高业务办理效率，还让贷款审批更加规范。

然而，仅仅开发了 APP 还不够，根据银监会和青岛银行的监管规范，这套移动业务系统需要保证信用风险管理系统的身份接入和数据的安全性。因此，青岛银行选择了深信服 SSL VPN 产品的应用安全加固解决方案。



将 VPN 的 SDK 代码集成进信用风险管理系统 APP 中，APP 在互联网上传输数据时不再是明文，同时支持安全性高的国密算法进行传输。此外，为了数据落地移动终端的安全性，应用安全加固方案还提供了数据存储加密的功能，防止移动终端上敏感数据的外泄。

