移动办公及业务应用
安全保障白皮书

中国网络安全产业联盟
2020 年 3 月

版 权 声 明

前　言

随着移动互联网的快速发展，个人消费类移动应用大量涌现并深深影响社会生活的同时，包括政府、金融、运营商、能源、交通等在内的各行业原有的业务/办公等应用服务也在逐步实现移动化，从传统面向PC终端提供办公和业务应用服务，扩展到了面向智能移动终端（手机/平板）提供服务，办公和业务应用移动化帮助行业机构摆脱时间和空间的限制，随时随地按需要处理工作，从而实现效率提升和协作增强。尤其在疫情期间，为了保障“一手抓抗疫，一手抓生产”，移动办公和业务应用成为众多企事业单位抗击疫情、复工复产的重要选择，为保护员工健康、稳定社会经济发挥了重要作用。

行业业务移动化，经历了从配发设备（COPE）到自携设备(BYOD)的使用模式变迁，也经历了从原生应用到原生/Web混合应用的技术形态发展，形成了众多移动业务应用场景。移动业务场景不仅面临着分布在云管端的多种安全威胁和风险，而且同时面临着国家和行业的网络安全监管合规要求，如何平衡好安全控制和用户使用体验，处理好安全控制和个人隐私保护的关系，能对网络安全风险进行有效控制，并且

确保符合监管合规的要求，是行业机构在业务移动化过程中普遍关注的焦点问题。

为此，中国网络安全产业联盟联合北京指掌易科技有限公司、中国移动通信集团有限公司等单位，共同编制了《移动办公及业务应用安全保障白皮书》，旨在为行业业务移动化进程中，面对移动业务场景安全保障需求，提供建设思路的指导和借鉴。限于研究时间和编者能力，部分白皮书内容难免存在纰漏，不足之处恳请业界同仁批评指正。

本白皮书梳理了移动办公及业务应用发展的现状，系统分析了移动办公和业务应用面临的安全风险，结合当前国家和行业的网络安全监管合规要求，提出了面向行业移动业务场景进行安全保障建设的整体思路，从安全技术和安全管理两个维度提供了可参考的控制措施体系设计，并介绍了主要安全技术，最后对移动办公及业务应用安全发展趋势做出了预测。本白皮书还选取了典型企业移动办公应用安全保障案例进行了重点介绍。

目 录

一、移动办公及业务应用发展现状

（一）移动互联网发展规模

移动互联网依托于移动通信网络基础设施、智能移动终端设备、以及创新移动应用等各方面技术进步，经过十余年的迅猛发展，已经深深渗透和影响到我国国民经济和社会生活的方方面面，被公认为第三次 IT 技术革命。

图 1 移动互联网发展历程

2007 年安卓操作系统和苹果 IPHONE 手机发布是移动互联时代开启的标志性事件，到 2012 年中国手机网民数量超过了 PC 网民数量，智能移动终端作为互联网流量入口的地位越来越凸显，2019 年 5G 移动通信网络投入商用，为移动互联网进一步发展提供了强劲的助力。

根据中国互联网络信息中心 CNNIC 第 43 次《中国互联网络发展状况统计报告》和第 44 次《中国互联网络发展状况统计报告》，移动互联网在我国蓬勃发展的规模得到了印证：

- 截至 2019 年 6 月，我国手机网民数量达到 8.47 亿，较 2018 年增加 2984 万，网民使用手机上网的比例达到 99.1%;
- 2019 年上半年我国移动互联网接入流量消费达到 553.9 亿 GB，同比增长 107.3%;
- 截至 2018 年 12 月，我国市场监测到的移动应用 APP 在架数量为 449 万款，其中国内第三方安卓应用商店移动应用数量 268 万款，占比为 59.7%，苹果商店（中国区）移动应用数量 181 万款，占比为 40.3%;
- 我国智能手机操作系统市场份额显示，安卓系统占比已经超过 80%。

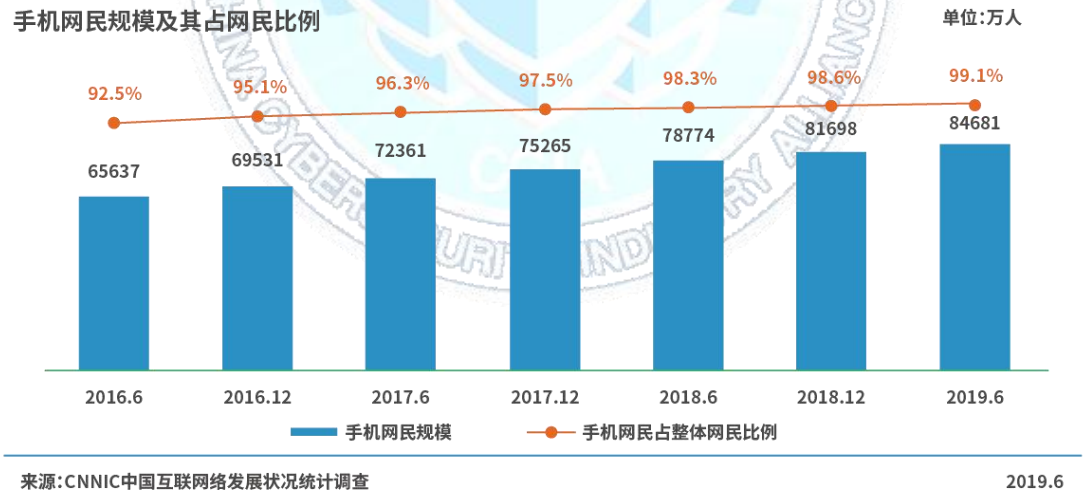

图 2 手机网民规模及其占网民比例

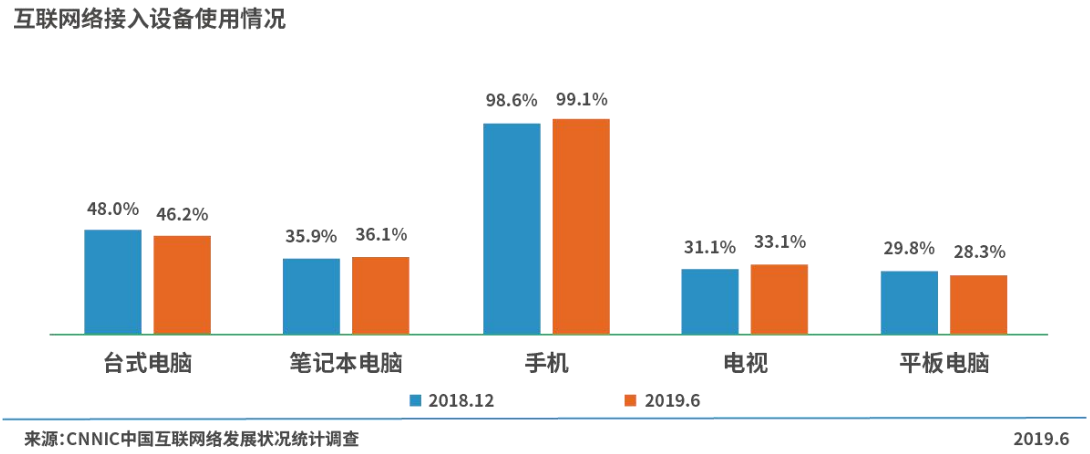

图 3 互联网络接入设备使用情况

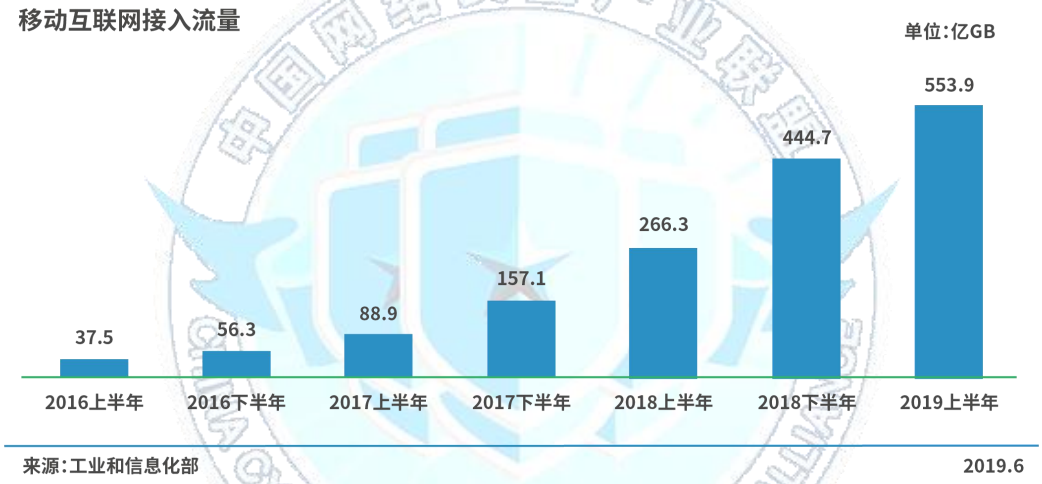

图 4 移动互联网接入流量

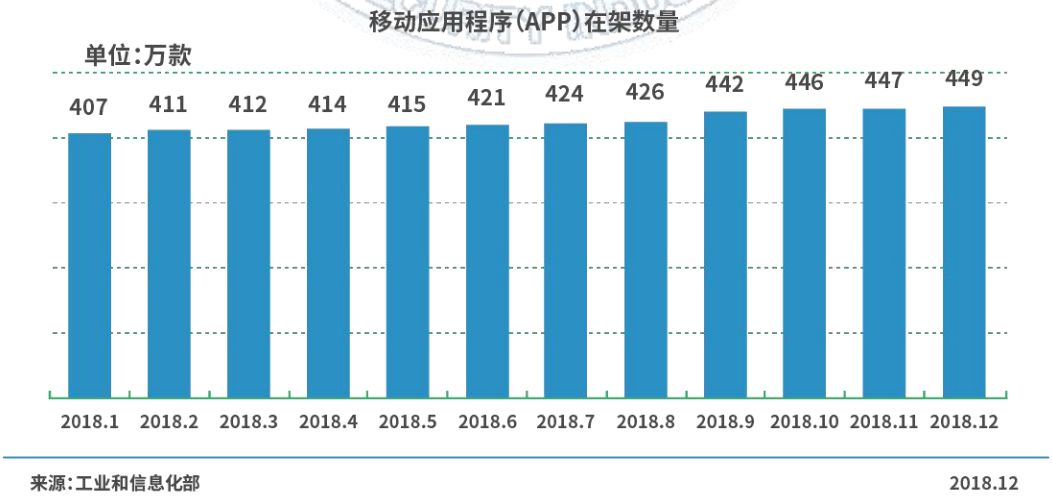

图 5 移动应用程序（APP）在架数量

（二）移动办公及业务应用发展现状

在移动互联网发展的大背景下，政府、金融、医疗、教育、制造、交通、能源、服务等各行业机构的内部办公和业务应用系统，也越来越多实现了移动化，从传统面向 PC 终端提供办公和业务应用服务，扩展到了面向智能移动终端（手机/平板）提供服务，办公和业务应用移动化能够帮助用户摆脱时间和空间的限制，随时随地按需要处理工作，从而实现效率提升和协作增强。

各行业的办公和业务应用移动化，在移动端主要体现为较为通用性的移动办公应用（如移动 OA、即时通讯、文件云盘、电子邮件等）、以及体现各行业特点的移动业务应用（如政府行业的无纸化会议、银行业的移动展业、房地产服务行业的移动经纪业务、物流服务企业的移动物流和仓储管理、能源电力行业的移动巡检和数据采集、制造业企业的 ERP 应用等）。

各行业移动办公和业务应用，在移动端的 APP 形态主要包括两类:

- 原生应用形态，通过自主/外包方式设计开发独立的原生应用，实现特定业务操作入口，政府、金融、运营商、企业等机构都广泛使用原生形态的移动应用，一

个行业机构常常为多种业务应用，开发多个原生应用，供用户在移动终端安装和使用;

- 基于门户应用的混合应用形态，部分政府、企业机构，依托政务钉钉、企业微信、蓝信、云之家等第三方门户应用，或者自主/外包方式开发的门户应用，在门户应用中嵌入实现特定业务操作的小程序/H5 轻应用，因为门户应用是原生应用，轻应用是 Web 应用，所以这种移动端 APP 被称为混合应用形态，即在应用客户端混合使用了 B/S 和 C/S 架构。

各行业机构的移动办公和业务应用的客户端 APP，其用户通常是机构的员工和合作伙伴人员，通常在分发渠道选择上，不会发布到公开应用市场，而是通过自建的私有应用市场进行发布和提供下载/更新,这样既能够实现对应用发布更灵活、更快速的管理控制，又能够规避应用发布到公开应用市场后所面临的逆向分析、篡改仿冒等恶意威胁。

（三）移动办公及业务应用的设备使用模式

用户要使用移动终端设备安装和操作移动办公及业务应用，移动设备使用模式，主要包括了企业配发设备（COPE）和员工自携设备（BYOD）两种常见类型:

- 企业配发设备（Corporate-Owned Personally Enabled,

COPE）模式往往被特定的行业移动应用推广所采用，行业机构为用户统一配发选定品牌型号的智能移动设备，本着专机专用的原则，仅能够在设备上使用行业应用，例如银行业的移动展业应用、政府行业的无纸化会议应用、能源行业的移动巡检应用中，配发设备仍然是主要的使用模式。该模式存在建设和维护成本高的局限，也具备适配简单的优点；

- 员工自携设备（Bring Your Own Devices，BYOD）模式正在被众多行业的移动办公和业务应用推广所采用，利用员工的个人移动设备，安装和使用移动办公和业务应用，可以节省大量的设备采购和维护投入，而且对用户来说，使用一台移动设备，可以同时满足个人生活和办公业务的使用需要，用户使用体验上效果较好。但因为个人设备类型的多样化，尤其是安卓设备的碎片化，需要应用能够处理好复杂的设备兼容性适配。

在部分国家政府机构的移动业务场景中，例如公安部门的移动警务、以及司法行政部门的移动执法等，还存在着一种特殊的双系统手机使用模式，兼顾考虑到业务场景的特殊管控要求、以及用户使用方便等因素，在一台智能移动手机

硬件设备上，使用安全容器技术手段隔离出两个完全独立的手机操作系统，其中生活系统可作为个人生活使用，出于个人隐私保护的考虑不进行安全管控，而工作系统，要确保符合特定执法场景的业务管控需求，必须按照专机专用的原则，安装终端安全监控组件，对设备、应用、数据等进行全方面的安全管控。

图 6 双系统移动执法终端

双系统手机以统一配发 COPE 模式发放给用户，但是仅对其中的工作系统进行特别管控，而生活系统则考虑了用户使用的方便，因此双系统手机使用模式，本质上是 COPE 模式，同时具备了 BYOD 模式的特点。

二、移动办公及业务应用面临的安全风险

行业机构建设和运营移动办公和业务应用，是一个覆盖“云、管、端”的完整互联网信息系统，包括了移动端的移

动 APP，数据中心的移动应用服务，以及移动端与应用服务之间的数据通信信道等组成部分。业务移动化在增强协作和提升效率的同时，也会面临着网络安全风险。

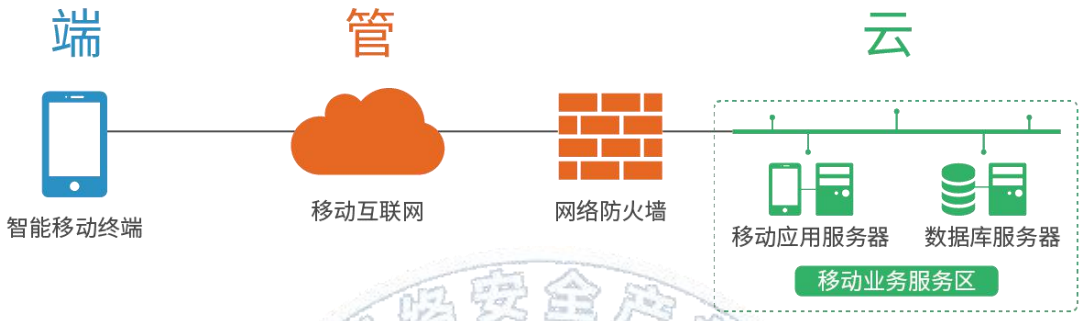

图 7 移动应用场景构成

互联网无处不在的安全威胁和安全风险，随时威胁着移动办公和业务应用的服务、数据等重要信息资产，虽然不同行业的移动业务应用本身具备各自鲜明的行业属性，但是从移动业务应用所面临的网络安全风险类型来看，又具备较高的相似性，可以暂且忽略行业属性的差异，针对移动办公和业务应用系统的云、管、端构成的通用场景，来对网络安全风险的具体体现进行分析。

（一）移动应用 APP 安全风险

安装运行在智能移动设备上的办公和业务应用 APP，面临着敏感信息泄露、应用仿冒、用户身份冒用、个人隐私侵犯等四类主要安全风险。

移动端的办公和业务信息泄露，是行业机构普遍关注的

重要风险，移动端敏感信息泄露，在以下情况可能发生:

- 移动应用用户通过截屏、复制/粘贴等操作，将办公和业务数据发送至外部应用，或分享到互联网;
- 移动设备上其它应用，访问获取移动办公和业务应用的数据;
- 员工离职或设备丢失，移动办公和业务数据仍然在移动设备上留存，可能被非法使用;
- 特殊时期（比如疫情期间），移动办公应用被安装在未经安全确认的移动设备上，移动设备上存在恶意应用，通过界面劫持攻击非法窃取移动办公和业务应用的数据。

任何通过公开应用市场发布的移动 APP 都会面临应用仿冒风险，该风险是指攻击者对原官方应用程序进行逆向分析后，对程序进行篡改或插入代码，二次打包后发布并诱骗用户进行下载安装，以隐私窃取、广告推送、恶意扣费等方式侵害用户利益，实现非法牟利。

身份冒用风险是指移动办公和业务应用的用户账户身份信息被破解或泄露后，合法用户的身份被非法冒用，攻击者冒充合法用户登录进入系统后，访问敏感数据资源。仅依靠用户名/静态口令的身份认证机制，移动办公和业务应用

系统很容易发生身份冒用。

个人隐私侵犯风险是指移动办公和业务应用 APP 具有过度索权的情况，超出自身业务功能需要，故意扩大移动应用的权限，违规采集和使用用户个人隐私信息，对用户个人信息构成危害和侵犯，违反了国家关于个人信息保护的法律法规。我国非常重视个人信息安全保护，《网络安全法》、GB/T 35273-2020《个人信息安全规范》等都对个人信息保护提出了明确的要求和相关依据，中央网信办、工信部、公安部、国家市场监督管理总局四部委在 2019 年联合成立“APP 专项治理工作组”，依法开展了“APP 违法违规收集使用个人信息专项治理行动”，对违规 APP 给予通报、下架等处罚。

表 1 移动 APP 安全风险

序号	风险	风险描述
1	信息泄露	移动办公和业务应用的敏感数据在移动端以主动或被动的方式不受控的对外泄露
2	应用仿冒	官方应用被恶意攻击者逆向分析和篡改，二次打包后重新发布，以钓鱼方式欺骗用户下载安装，达到恶意目的
3	身份冒用	恶意攻击者冒充合法用户身份访问移动办公和业务应用服务，非法访问敏感数据资源
4	个人隐私侵犯	移动办公和业务应用，超过业务需要，过度采集使用用户个人隐私信息

（二）移动应用通信安全风险

从移动端到服务端之间的通信，会通过移动互联网（运营商移动接入网络或无线 WIFI，以及有线互联网部分）进行，

在开放公众网络中，恶意威胁和风险水平较高，因此数据通信过程中，同样会面对通信窃听导致敏感信息泄露的风险和非法篡改通信内容危害通信完整性的风险，尤其是行业机构的移动办公和业务应用系统，因为处理和传输的业务数据敏感级别比个人消费应用更高，一旦发生信息窃取或篡改，往往造成更加严重的不良影响。

表 2 通信安全风险

序号	风险	风险描述
1	通信内容窃听篡改	通过恶意 WIFI 接入、网络通信嗅探等手段，对移动办公和业务应用的通信内容进行截获，从中窃取敏感信息（如登录账户信息、敏感文件和业务数据等），或对通信内容进行篡改。

（三）移动应用服务端安全风险

移动办公和业务应用的服务端，往往是部署在数据中心内部的核心信息资产，包括了 Web 服务器、应用服务器、数据库服务器、数据存储设备等，数据中心的形态可能是私有数据中心、云计算数据中心、或者未来的边缘计算中心，也可能是现有的传统物理形态数据中心，或者云计算中心。

数据中心的信息资产会面临与传统互联网应用相似的网络安全风险，包括拒绝服务、入侵攻击、恶意代码、越权操作、以及单点故障等，会危及到移动办公和业务应用系统的服务可用性、基础运行环境的完整性、以及业务数据的机

密性和完整性，这些服务端的网络安全风险需要通过传统网络安全机制进行有效控制。

表 3 服务端安全风险

序号	风险	风险描述
1	单点故障	服务端应用节点（如 Web 服务器、App 服务器、DB 服务器、负载均衡设备等)及所在网络环境中的网络节点(如交换机、路由器、防火墙等）发生故障，造成移动办公和业务应用系统服务中断。
2	拒绝服务	来自于互联网环境的流量型或应用型 DoS/DDoS 攻击，恶意消耗服务端资源（线路带宽、服务器 CPU 和内存、服务器网络连接资源等），造成移动办公和业务应用系统服务性能下降或服务不可用。
3	入侵攻击	服务端基础运行环境（含操作系统、数据库、中间件等），以及应用程序存在可被利用的未修复安全漏洞，攻击者实施攻击后可非法提权，实现数据窃取和篡改。
4	恶意代码	服务端基础运行环境（含操作系统、数据库、中间件等），以及应用程序存在可被利用的未修复安全漏洞，感染蠕虫病毒、勒索病毒、或恶意木马程序，造成服务中断、信息泄露等结果。
5	越权操作	特权管理账号弱口令、应用访问控制的权限管理不严格、或鉴权机制存在逻辑漏洞可被绕过，导致攻击者或用户获得非法的操作权限。
6	数据损失	因发生环境灾难事件，缺乏数据冗余存储和备份机制，导致数据不可恢复受损。

在 SaaS 移动办公场景中，还存在一种特殊的、涉及云服务商的数据安全风险，即租户方的内部办公数据因储存在云端，可能被云服务商非法获取和使用的风险，如果移动办公服务端的 IT 设施部署运行在私有化环境中，这种风险并不存在，但是在 SaaS 移动办公场景中，往往成为租户方特别关注的重点，市场上有第三方的数据加密方案，能够对这

种数据安全风险进行控制。

以上广泛存在的网络安全风险，威胁着移动办公和业务应用系统的服务可用性/完整性，以及业务数据的机密性/完整性/可用性等安全属性，安全保障建设的目标首先是对系统所面临的主要安全风险进行全面有效的控制，因此进行安全风险的识别和评估分析是保障移动办公和业务系统安全运营的必要前提条件。

三、移动办公及业务应用安全监管要求

网络安全监管合规要求，既可以为各行业机构的安全保障实践活动提供思路和方法上的借鉴和指导，又是应当满足的控制措施内容，因为在信息安全管理体系中，合规性管理也是一类重要的管理机制。

移动业务场景是随着移动互联网发展起来的较新领域，目前针对移动业务场景的安全保障，从国家、到行业、再到企业，都已经着手建立相关的安全技术规范，不同层面在标准规范方面的投入，都是面向移动安全领域非常重要和宝贵的管理实践活动。

（一）国家标准

1. 等级保护 2.0 移动互联安全扩展要求

GB/T 22239-2019《网络安全等级保护基本要求》为了便于实现对不同级别和不同形态的等级保护对象的共性化和个性化保护，GB/T 22239-2019《网络安全等级保护基本要求》在提出安全通用要求的同时，针对云计算、移动互联、物联网、工业控制系统提出了安全扩展要求。其中明确规定，采用移动互联技术的等级保护对象其移动互联部分由移动终端、移动应用和无线网络三部分组成。GB/T 22239-2019移动互联安全扩展要求主要针对移动终端、移动应用和无线网络部分提出特殊安全要求，与通用要求一起构成对采用移动互联技术的等级保护对象的完整安全要求。

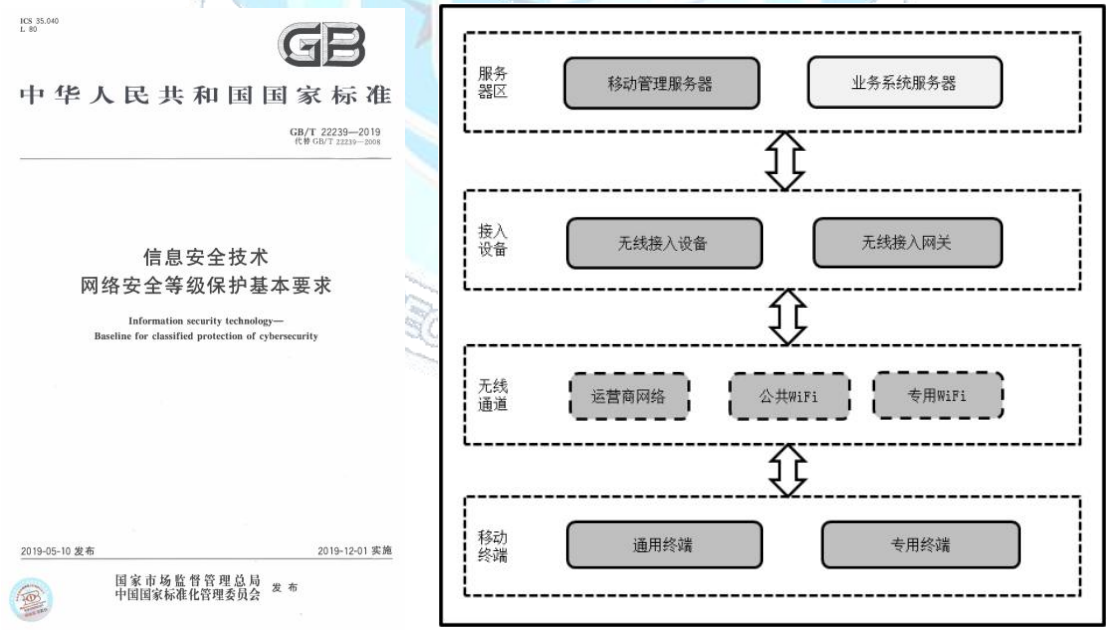

图 8 等级保护 2.0 的移动互联场景

以 GB/T 22239-2019 中三级定级对象的移动互联扩展要求为例，一共包括了 9 个控制点，其中 5 个控制点与无线网

络安全有关，4 个控制点与移动终端和移动应用安全有关，其结构如下表所示：

表 4 等级保护 2.0 移动互联安全扩展要求

无线网络相关控制点	移动终端/移动应用相关控制点
无线接入点的物理位置	移动终端管控
边界防护	移动应用管控
访问控制	移动应用软件采购
入侵防范	移动应用软件开发
配置管理	

2. 移动智能终端安全架构

GB/T 23927-2016《信息安全技术 移动智能终端安全架构》提出了智能移动终端的安全框架，由硬件安全、系统软件安全、应用软件安全、接口安全、及用户数据安全五部分组成，如下图所示：

图 9 智能移动终端的安全框架图

在应用软件安全方面，标准描述了最小权限原则、安全扫描、应用安装、安全软件等四项安全需求，在用户数据安全方面，标准描述了远程保护、状态提示、用户确认、信息保护、信息收集、文件分级等六项安全需求。

（二）行业标准

1. 金融行业

中国人民银行 2019 年发布了 JR/T 0092-2019《移动金融客户端应用软件安全管理规范》，面向金融行业在移动端开展的资金采集、资讯查询、信息采集等类型的应用软件，从身份认证、逻辑安全、安全功能设计、密码算法和密钥管理、数据安全等五个方面提出安全技术要求，从设计、开发、发布、维护四个阶段提出安全管理要求，以规范金融行业移动应用客户端软件的安全保障。

2. 电信行业

运营商是移动通信网络服务的提供者，作为电信行业的主管机构，工信部牵头制定了一系列的通信行业标准规范，包括 YD/T 3082-2016《移动智能终端个人信息保护技术要求》、YD/T 3039-2016《移动智能终端应用软件安全技术要求》、YD/T 2407-2013《移动智能终端安全能力技术要求》、YD/T 2439-2012《移动互联网恶意程序描述格式》、YD/T 2408-2013《移动智能终端安全能力测试方法》等，这些通信行业标准是国内制定的较早的面向移动互联网领域制定的标准规范。

3. 公安行业

公安部在 2018 年针对警务业务场景中使用的智能手机

型移动警务终端，发布了 GA/T 1466.1-2018《智能手机型移动警务终端 第 1 部分：技术要求》和 GA/T 1466.2-2018《智能手机型移动警务终端 第 2 部分：安全监控组件技术规范》等公安行业标准，对双系统警务终端的硬件设备、操作系统、以及用于终端安全管控的安全监控组件提出了全面细致的技术要求。

其中对安全监控组件的技术要求包括了运行环境、一般要求、功能要求、性能要求、以及接口要求等部分，尤其是安全监控组件对移动警务终端的安全管控能力要求包括硬件模块管控、终端基本功能管控、终端应用管控、监测采集管控、系统使用模式管控、管控策略围栏、远程控制和配置、升级等多个方面。

安装了安全监控组件的双系统移动警务终端必须符合 GA/T 1466 公安行业标准，并通过检验认证，才能够在公安行业内销售和使用。

4. 司法行政行业

司法部牵头制定和发布国家司法行政行业标准，在 2018 年发布的 SF/T 0028-2018《智慧监狱技术规范》中，明确对司法行政业务场景中使用的移动执法终端提出了技术要求，涉及工作模式、专用系统版本、安全监控组件、移动执法应

用等方面。

仍在制定中的《司法行政移动执法系统技术规范》中，全面针对移动执法的业务场景，从双系统移动执法终端、终端安全监控组件、移动执法网络接入、移动执法组网、移动执法应用开发、移动应用市场、即时通讯软件等方面提出了具体技术要求，该规范适用于全国范围内司法行政和监狱/戒毒所等单位的移动执法系统建设。

（三）企业标准

1. 中国移动

中国移动在业内率先发布了《重大突发公共卫生事件网信安全法律风险合规指引》，从法律合规角度提出了业务、数据等安全风险管控建议；制定实施了《中国移动业务安全通用评估规范》、《中国移动移动智能终端软件安全要求》等系列企业标准，对互联网业务、移动智能终端软件应遵从的安全要求进行了规定，包括应遵从的安全原则、能力调用安全要求、资源访问安全要求、网络访问安全要求、业务相关安全要求和应用软件服务后台安全要求等；基于企业标准实施了《云端联动的隐私安全防护体系及公益服务》项目，荣获联合国 2020 年信息社会世界峰会（WSIS）“杰出项目奖”，标志着我国的移动业务应用安全方案获得国际认可。

2. 中国电信

中国电信制定了《IT 安全规范及示范细则要求》的企业标准，其中针对移动 APP 统一接入提出了具体的技术要求，包括具备认证管理、数据安全传输、应用数据安全隔离、应用安全管理（应用商店）、安全审计功能，实现移动应用传输通道加密、APP 内数据安全隔离及原应用无需改造的安全发布功能，逐步实现单点登录等细化内容。

3. 中国铁路总公司

中国铁路总公司制定了《铁路移动互联网智能终端安全接入平台技术条件》的企业标准，从智能移动终端安全、传输安全、接入安全、应用安全管理、应用集成接口、运维管理、安全审计等七个方面提出了安全功能和性能方面具体细化的技术要求。

四、移动办公及业务应用安全保障实践

（一）实践领域的发展变化

1. 个人应用 APP 加固

移动互联网的发展，首先推动了个人消费领域的移动应用发展，各种面向个人消费者的 ToC（To Customer）应用，首先会面临利用漏洞攻击和二次打包的安全威胁，所以围绕

移动 APP 进行漏洞检测和加固成为最受关注的重点。

通过工具扫描和人工渗透测试等手段，发现并修补移动 APP 所存在的安全漏洞（例如信息泄露漏洞、注入漏洞、处理逻辑漏洞等），并且通过 APP 加壳手段，使得对外发布的移动 APP 具备反调试、反逆向、反插入篡改等能力，确保恶意攻击者利用漏洞进行攻击、对移动 APP 通过逆向分析和调试插入等操作进行二次打包等威胁相关联的安全风险得到有效控制，从而保障移动应用服务稳定可靠运行、个人用户信息和财产安全。

2. 移动设备管理（MDM）和企业移动管理（EMM）

依托移动互联网发展的行业业务移动应用，使用者往往不是外部用户，而是企业的员工，所以可称作 ToE（To Employee）应用，此类应用场景在初期主要是 COPE 企业配发设备模式，以移动设备管理 MDM 为基础，实现了资产管理、用户管理、设备级策略管理等能力，而后参考 Gartner 的企业移动管理套件 EMM 的定义，扩展出移动应用管理 MAM，移动内容管理 MCM 等能力，实现了面向移动应用和数据的生命周期管理和安全策略管理。EMM 方案目前仍在 COPE 使用模式的移动化业务场景中被使用。

基于 MDM 的 EMM 方案，由于安卓和 IOS 系统都提供可供

调用的系统级 API 接口，所以在具体的技术实践上，安全管控能力方面基本没有难点，重点需要处理好实际存在的安卓设备碎片化的适配工作，较为成熟的技术方案能够对不同版本的安卓系统、不同类型的安卓设备提供较好的兼容适配能力。

EMM 的基础是 MDM，能够较好地适应 COPE 模式，但是当越来越多的基于 BYOD 模式的移动业务场景出现之后，设备级安全管控与 BYOD 用户个人隐私保护之间就存在着难以调和的矛盾。

3. BYOD 模式的应用和数据安全

使用应用级安全容器技术的解决方案，实现了面向应用和数据的安全管控，通过容器来隔离和保障业务相关的移动 APP 和数据，与 BYOD 设备上的个人应用和数据分离，同时兼顾了业务保障和隐私保护，在越来越多的 BYOD 模式的移动业务场景中，此类解决方案逐渐得到了广泛的重视和使用。

面向移动应用和数据的安全管控方案，在应用安全容器的具体技术实现上，存在着稳定性、应用适配性方面的差异，尤其是在开源的安卓系统上安全容器所能够实现的安全管控能力，会明显优于封闭的苹果 IOS 系统上安全容器所能实现的能力。应用安全容器的技术优化和管控能力积累，是评

价此类方案能否较好适应复杂使用场景的关键因素。

4. 多模式融合方案

在较为复杂的使用场景中，同时存在着 COPE 企业配发和 BYOD 用户自携两种使用模式，目前已有能够较好兼顾不同使用模式的融合解决方案出现，既能够对专用配发设备及应用提供设备级安全管控，又能够对用户自携设备上的应用和数据提供应用级安全管控，此类方案未来会成为主要的实践趋势。

（二）典型行业移动办公及业务应用安全保障解析

1. 金融行业业务应用安全保障解析

以银行机构为代表的金融行业，往往具备相对复杂的移动业务场景，除去面向外部用户的手机银行 B2C 应用之外，还有众多面向员工的 B2E 应用场景，既有 COPE 的移动展业业务场景，银行客户经理使用统一配发的平板设备，到企业客户现场，完成以信贷业务为代表的业务开展活动，又有 BYOD 的移动办公场景，行内员工使用个人手机，完成电子邮件、移动 OA 等移动办公操作。银行机构对于不同的移动业务场景，有不同的安全保障需求。

对于手机银行为代表的 B2C 应用，重点需求包括:

- 对发布到公开应用市场的业务 APP 进行加固，具备抗逆向、抗调试、抗篡改能力，有效应对二次打包的威胁;
- 对各发布渠道的业务 APP 下载使用情况，以及仿冒 APP 的分布情况进行有效监测。

对于 COPE 的移动展业，重点需求包括:

- 配发设备的统一管理，包括了资产管理、设备策略管理、远程数据擦除等;
- 展业应用的生命周期管理，包括应用容器化、应用发布、推送、更新等。

对于 BYOD 的移动办公，重点需求包括:

- 移动端的工作域与个人域有效隔离;
- 移动办公数据的传输和存储安全;
- 移动端敏感信息防泄密;
- 移动应用与现有统一身份管理平台的认证集成;
- 办公应用的生命周期管理，包括应用容器化、发布、推送、更新等。

以某城商行机构为例，其实践方案包括了以下主要内容:

表 5 某城商行机构方案

移动业务场景	实践内容

手机银行应用服务	采购 APP 加固和 APP 分发渠道监测服务，确保发布的手机银行 APP 无严重安全漏洞，具备抗二次打包能力，且被合法的分发和使用。
移动展业应用服务	部署移动安全管理平台，实现移动设备管理、设备策略管理、企业应用市场、应用容器化、应用策略管理等能力，部署移动接入网关，实现认证准入、安全通信等能力。
移动办公应用服务	部署移动安全管理平台，实现企业应用市场、应用容器化、应用策略（移动端 DLP）管理等能力，通过与行内原有统一身份管理平台对接，实现用户同步、身份认证、和单点登录等能力，部署移动接入网关，实现认证准入和安全通信能力。

该银行的手机银行和移动展业业务场景，在经过安全保障建设之后，均通过了等级保护 3 级系统测评（等级保护 1.0 标准）。

2. 政府机构移动安全保障解析

政府机构普遍开展了办公业务移动化建设，以综合办公系统为代表的政务外网关键应用实现了移动化，通常以 BYOD 自携设备方式，下载并使用移动办公应用 APP。

政府机构对于移动办公业务场景的安全保障，有如下重点需求：

- 建立私有应用市场，进行移动办公 APP 的生命周期管理；
- 移动安全管理平台能够贴合政府委办局的组织架构，支持分级管理；
- 移动应用需要支持多种形式的双因素强身份认证，并且与现有统一身份管理平台进行集成，实现 SSO 单点登录；
- 移动端设备实现工作空间与个人空间的有效隔离；

- 移动端防敏感信息泄露;
- 移动端与移动服务端之间实现安全通信,且支持使用国密算法;
- 移动业务场景实现日志审计,并且通过标准接口,将审计日志数据报送到安全运营大数据分析平台,进行集中存储、分析和可视化呈现。

以某部委级政府机构为例,该机构面向覆盖部委和下级直属机构的移动办公场景,进行安全保障实践,建立了统一的移动安全管理平台,支持分级管理,内置企业级应用市场,对移动办公 APP 进行容器化,并进行发布、推送、更新管理。移动安全管理平台实现了与统一身份管理平台的对接,并实现了强身份认证和单点登录,另外实现了与安全运营大数据分析平台的数据报送。

在该部委数据中心和下级直属机构数据中心的移动应用服务之前进行了移动接入网关的分布式部署,确保从移动端到移动接入网关之间,通过移动互联网进行的数据传输得到加密和完整性保护,加密算法支持 SM1/SM2/SM3/SM4 等国密算法,符合政府机构的密码管理规定。

在移动端使用安全工作空间隔离工作域与个人域,确保办公应用和数据只能在办公空间内被使用,移动端的数据存

储以加密机制保障，安全工作空间内部，各经过安全容器保护的办公和业务 APP，接受并执行由移动安全管理平台制定下发的安全策略，重点实现了移动端 DLP 防护能力，有效控制了政府公文从移动端泄露的安全风险

3. 物流行业移动办公安全保障解析

物流行业是社会经济生活的重要支撑性行业，其核心业务为快递业务，为了适应快递业务场景，并提高业务效率，大型物流服务公司均全面实现了速递业务场景的移动化，在移动端开发了支撑物流快递业务的移动业务 APP，数以万计的员工及外包合作伙伴使用智能移动端的应用，参与和完成快递业务。

在快递业务的移动化场景中，往往使用企业配发设备 COPE 模式，为业务人员统一配备了专用手机，在使用场景中对业务人员使用的移动设备具有以下的管理需求:

- 对移动设备进行统一的资产管理和策略管理;
- 不允许设备使用者随意安装其他个人应用，控制移动设备运行环境因不可控应用安装运行产生的安全风险;
- 对移动设备上的物流业务应用进行统一的发布、推送、安装、更新等管理;
- 对移动设备进行统一监控，实时获取设备电量、信号

强度、物理位置等数据;

- 对移动设备进行业务数据采集、集中分析、可视化呈现，为业务感知和优化决策提供支撑。

以某国内龙头物流服务企业为例，该企业的快递业务移动化场景，使用了 EMM 移动安全解决方案，在业务移动设备中预置/安装了 EMM 客户端，在数据中心建立 EMM 移动安全管理平台，覆盖了 3w+规模的设备和用户，具备了以下管理能力:

- 实现了对移动设备的统一管理，包括了资产注册、设备策略、资产状态和使用监控、设备远程操作、资产管理报表输出等功能，让管理人员可以统一定制设备策略、了解所有移动设备的运行使用情况，在发生可疑或异常情况时，可以远程进行数据擦除等管理操作;
- 通过在移动设备进行数据采集，在管理后台可以对业务人员的工作轨迹、通话记录（含通话录音）、短信/彩信记录等数据，进行集中审计分析，方便管理人员实时了解业务人员的工作状态;
- 建立企业级私有应用商店，对业务应用 APP 进行发布、推送、更新、下架等完整应用生命周期统一管理，管理后台可以对发布安装的业务应用定制下发安全策略，

对业务数据提供移动端防泄密等保护;

- 提供设备管理的远程协助，对业务人员反馈的移动设备使用问题进行快速响应、定位和解决，协助运维管理人员简化技术支持操作，提高运维支持效率;
- 移动设备采集的数据，快速对接企业业务大数据分析平台，按照管理需求进行综合分析和可视化呈现，有力支撑快递业务监控和优化管理。

4. 房地产服务行业移动办公安全保障解析

随着我国经济发展，房地产服务行业蓬勃发展，为用户提供房地产租赁、买卖等过程的经纪服务，经纪服务业务已普遍实现了信息化和移动化，往往以员工自携设备 BYOD 的模式，在个人智能手机上使用经纪服务 APP 进行业务操作。

对房地产经纪服务机构来说，企业的核心数字资产就是房地产经纪服务过程中不断积累的房源、买卖双方、出租/承租双方等信息，如果在移动端没有对这些数据信息提供安全保护能力，随时可能发生业务人员将移动端获取的房源信息、客户信息等通过买卖实现非法获利的情况，给正常业务开展造成损失。

例如，某国内房地产经纪服务的龙头企业，旗下有超过五万名房地产经纪人，该企业采用了移动业务数据安全解决

方案，解决目前移动业务场景中的数据安全风险，方案包括两方面内容:

- 为经纪服务 APP,提供移动端数据防泄密的 SDK,该 SDK 内置了禁止应用截屏操作、禁止应用中的复制/粘贴操作、以及应用水印等能力，集成了防泄密 SDK 之后，经纪人用户将不能在使用过程中，通过复制粘贴和截屏等操作，将房源、客户等敏感业务信息轻易获取和外泄，从而对该企业的核心数据资产保护提供了有力支撑;
- 在企业数据中心互联网边界建立了移动安全接入网关，一方面移动 APP 到数据中心之间的数据传输进行了高强度加密保护，恶意攻击者不能够利用通信窃听等手段非法获取敏感业务信息，另一方面，接入网关前置，将应用服务器移至网关后端，接入网关提供的认证准入和通信转发等控制功能，能够明显降低应用服务被来自互联网的恶意攻击者入侵、攻陷的安全风险，进一步增强了对数据中心重要服务资产的安全保护。

五、移动办公及业务应用安全保障设计

（一）移动办公及业务应用安全保障思路

在面向多种移动办公及移动业务应用，进行统一的移动安全保障体系的设计和实施时，我们建议按照安全工程的规范方法，结合 BYOD 发展趋势和个人信息保护政策要求，基于准确的网络安全风险识别与评估结果，对移动安全技术和管理控制措施进行体系化设计，然后选择能满足设计要求的产品方案，按照具体移动应用场景的需要制定并执行细化安全策略，以实现风险控制和监管合规的双重目标，主要包括以下七个步骤。

(1) 面向 BYOD 个人自携设备的场景实现业务移动化和安全保障。

基于 BYOD 场景的业务移动化，具备最佳的用户使用体验和最低的系统建设成本，根据 Garter 的统计，2019 年所有业务移动化场景中，BYOD 场景占比已经超过了 60%，且是未来必然发展趋势，COPE 配发设备场景仍然还会存在于特定的行业移动化场景中，但不构成主流趋势。

(2) 以移动应用为中心提供安全保障，兼顾安全控制与用户体验的平衡。

基于 BYOD 场景，移动安全控制的重点将从之前的移动

设备管理转移到移动应用管理，安全控制将兼顾用户使用体验和用户隐私保护，与移动应用相融合。

(3) 面向移动业务场景的安全风险和合规要求，选择和组合安全控制能力。

对移动业务场景中分布在云管端的安全风险进行识别和评估，同时对国家网络安全监管面向移动业务场景的合规要求进行分析，然后确定移动安全保障的有效安全需求，根据安全需求选择和组合对应的安全控制能力，形成安全控制能力体系的设计。依据以上过程形成的安全能力体系设计，既能够对主要安全风险提供有效控制，又能够确保符合监管合规的要求。

(4) 确定安全控制能力与移动应用相结合的技术路线。

在安全能力体系设计基础之上，需要在不同解决方案供应商的产品技术路线之间进行比较和选择，应优先选择能够实现快速安全赋能的技术路线，尤其是移动端安全赋能，不同的技术路线方案，在适应移动业务场景的快速迭代交付时表现出来的能力，存在一定的差异。

(5) 结合移动业务场景制定安全控制策略。

完成移动安全保障方案的部署后，在面向特定的移动应用进行安全控制时，应细化制定灵活的安全控制策略，使得

特定的安全控制能力能够贴合具体业务场景的需要，更好地与应用相融合。管理平台制定的安全控制策略，要能够及时下发至移动端生效。

(6) 积累移动业务场景安全运营数据，提升整体感知和运营优化能力。

因为移动端安全能力组件具备移动端数据采集上报能力，所以基于业务需要，在不违反国家关于个人信息安全保护要求的条件下，合理合法采集安全及业务运营数据，上报至管理平台进行集中存储和分析利用，以期提升移动业务场景的安全感知能力和业务运营优化能力。

(7) 履行网络安全监管合规的职责和义务。

在移动业务场景的运营过程中，还需要履行国家网络安全监管对网络服务运营者规定的职责和义务，包括等级保护定级备案、个人信息安全保护、安全迎检和系统测评等。

（二）移动办公及业务应用安全控制体系

移动办公及业务应用的安全保障目标，最终需要落地安全控制措施来实现，在此过程中，应遵循两个基本的原则：

- 三同步原则，即安全与应用的同步规划、同步建设、同步使用原则，在业务移动化过程中，同步进行配套安全保障机制的建设，既能够使建设代价降低，又能够减少

移动应用安全风险暴露级别;

- 技术管理并重原则，自动化的安全技术措施必不可少，可以高效准确地提升安全风险控制能力,然而同时应当重视安全管理机制的建设,与技术措施一起形成整体保障体系。

1. 安全技术控制

参照国家相关标准和行业最佳实践经验，移动办公和业务应用保障的安全技术控制措施，应当考虑:

- 访问控制措施，包括了基本的身份认证机制，至少两种身份认证机制组合形成的强身份认证手段，应用与设备认证绑定后的准入控制，方便易操作的统一身份认证和单点登录SSO,另外还包括基于移动端安全风险持续监测，并根据监测结果动态调整准入策略的零信任安全措施;
- 数据安全措施，包括了移动端对移动应用和数据提供本地环境隔离保护的应用级容器，本地数据文件加密存储和配套秘钥管理机制，移动端数据防泄漏，以及移动端与服务端之间的应用级加密通信，另外需要注意的是，对于重要的等级保护对象或重点行业的移动应用数据保护，监管标准还要求数据传输和存储环节

使用的加密算法类型不仅应支持国际标准算法，还要能够支持国密算法;

- 安全审计，安全审计是安全运营的有力支撑措施，移动办公和移动业务应用场景中的安全审计要求能够对移动应用的用户操作、特权管理角色的管理操作、甚至移动应用的内容进行数据采集和审计记录，审计日志数据的格式/内容/保持期限等，以及对审计数据和审计进程要求符合国家网络安全监管标准的要求，另外安全审计数据在运营过程中的积累，也能够为数据分析和安全态势感知能力提供主要的数据源支撑;
- 移动应用安全加固，包括两个方面，一方面是移动应用自身的安全脆弱性检测和修补，往往通过自动化的安全漏洞扫描和人工渗透测试等工具方法完成安全脆弱性的识别检测，然后进行代码修改实现脆弱性加固，另一方面是对抗移动应用面临的逆向、调试、篡改等恶意安全威胁的能力，通过应用加壳加固的技术手段实现，此项能力对那些通过公开应用市场发布的移动办公和移动业务应用来说尤其重要;
- 安全分析和感知，当移动应用数量较多、用户规模较大时，安全运营过程需要安全数据分析和态势感知能

力的有力支撑，在安全审计机制积累的安全运营数据，以及移动端数据采集能力的基础上，对安全运营数据进行集中存储和分析挖掘，能够更精准地了解运营过程中的安全风险/事件，提升应急处置等运营保障工作的效率；

- 移动安全管理服务，体系设计、应急响应、安全测试、监管合规等安全管理过程的落地，需要必要的技术服务手段予以支撑，这些手段往往通过服务采购的方式实现；
- 移动应用生命周期管控，建立企业级移动应用门户，管理移动应用生命周期的加固赋能打包、发布、下载、更新等环节，既可以降低公开应用市场发布的篡改/仿冒风险，又能够实现便捷的安全加固赋能，提升用户使用体验；
- 其他可扩展机制，移动业务场景，以及伴随的安全威胁、安全漏洞、安全风险都是在快速发展变化的，国家网络安全监管也可能为适应发展提出新的要求，就要求移动应用安全保障技术体系具备开放性和可扩展性，能够补充增加进新的安全控制能力和措施。

图 10 移动安全技术控制

2. 安全管理措施

移动办公和业务应用的整体安全保障，还需要与技术控制措施并列的安全管理机制，因为安全保障本质上是一个 PDCA 的管理过程，不仅选择哪些技术措施需要管理过程进行

决策，而且在移动应用的开发/投产/运营的生命周期各阶段也需要有配套的安全管理策略和制度实现覆盖和指导。参考中国网络安全产业联盟正在制定的《移动互联网应用程序安全规范》，移动应用的安全管理措施可包括:

- 组织/人员安全管理制度，对移动业务场景进行安全管理的组织架构、岗位职责、人员配备、人员能力等阐述明确的管理要求和规定;
- 移动应用生命周期各阶段安全管理制度，移动生命周期中的设计开发、交付投产、运行维护等关键阶段，需要有对应的安全管理制度覆盖，而且为了保证安全管理制度得到有效的落地执行，还需要将安全管理制度的要求融合入各阶段主要工作流程和制度中，例如设计开发阶段，本着安全与应用建设使用三同步原则，就要求在风险分析、需求分析、系统设计、软件开发、软件测试等具体工作任务中，将业务部分与安全部分同步进行，还需要在开发设计阶段的工作流程中各关键评审节点，将安全部分的评审也作为重要评审内容加以规定。另外，在移动应用系统运行维护阶段要有各项相关的安全管理制度覆盖具体的工作场景，例如变更操作的安全要求，以及发生安全事件后的应急处

置过程管理等;

- 安全合规管理制度，包括了等级保护监管合规要求的定级备案、实施、测评等职责，以及个人信息安全规范要求的对个人信息采集使用应遵守的义务，这都要求有明确的管理策略和制度指导具体的工作。

图 11 移动安全管理措施

（三）移动办公及业务应用安全保障关键技术

1. 身份管理和身份认证

(1) 身份认证技术

身份认证技术，也称身份鉴别技术，保证访问主体身份真实性，是进行访问控制，以至确保数据安全性的关键基础技术，从技术机制分类上可分为所知、所有、所是三类，例如用户名/口令认证机制属于所知类型，硬件动态令牌属于

所有类型，指纹识别属于所是类型，将以上任意两种类型结合起来的身份认证机制被称为双因素认证机制。

传统 PC 互联网的用户身份认证，主要经历了用户名/口令、用户名口令+动态口令（含短信验证码）、用户名/密码+USBKey 等几代技术发展，通过双因素/多因素认证来提升身份认证机制本身的强度。

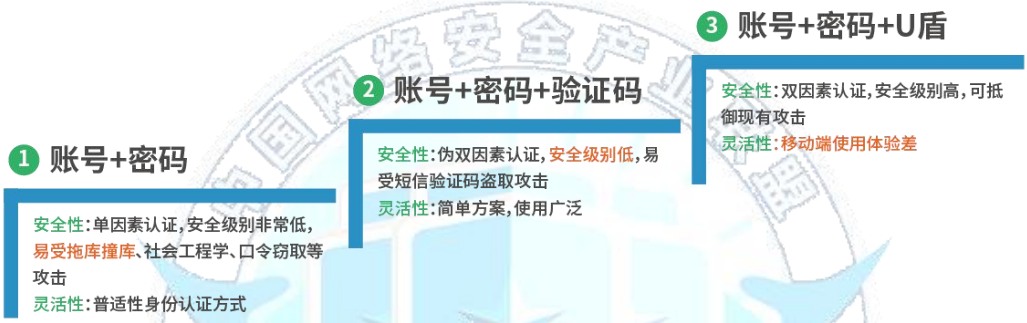

图 12 身份认证机制的发展

(2) 移动端身份认证技术

移动互联应用的用户身份认证，一方面与 PC 互联网应用类似，仍然会使用简单的用户名/口令认证，或者用户名/口令+短信验证码双因素认证机制，另一方面依托于智能移动终端设备的技术发展，使一些新型身份认证技术得到了更加广泛成功的应用，这些新认证机制包括:

- 手势密码，利用了移动终端的触摸屏，设置一笔连成的九宫格图案作为登录密码，只有输入的手势密码和设置密码完全相同时，才能够通过认证完成登录，该

机制本质上仍然属于所知类型的认证技术，只是相对于密码输入来说在移动端上操作更加简便快捷;

- 指纹识别/面部识别，利用了移动终端本身的指纹识别/面部技术，以实现基于生物特征的身份认证，无论是安卓还是 IOS，都将移动设备自身的指纹识别/面部识别认证能力提供 API 开放给移动端应用 APP，应用 APP 可以调用相应的 API 接口向移动操作系统申请本地认证服务，并获取认证结果，根据认证结果决定是否允许用户登录;
- 移动数字证书认证，传统 PC 端使用的数字证书+USB Key 安全性最高，但是要在满足移动端易用性前提下使用，需要在形式上有所变化，一种形式是将 PC 端使用的 USB 接口的 USB Key 进化为支持蓝牙协议的 USB Key，移动终端可以通过蓝牙无线协议与 USB Key 之间进行通信，实现数字证书获取和数字签名功能。第二种形式是将移动设备作为数字证书和私钥的载体，与 PC 端应用集成，为关键业务操作提供数字签名机制，第三种形式是将移动 SIM 卡（SIM 盾）作为数字证书和私钥的载体，与客户端应用集成，为关键业务操作提供数字签名机制。以上三种形式的移动数字证书认证目前

在政府、银行业已经有了应用。

(3) 统一身份认证和单点登录

在移动办公和移动业务场景中，尤其当存在多个移动业务应用时，通常需要综合安全性和易用性考虑，实现跨应用的 IAM 统一身份和认证管理，以及 SSO 单点登录特性。

很多企业用户已经建立了内部的统一身份和认证管理系统，用于实现集中身份管理和身份认证服务，最常见的形式就是 Linux 的 LDAP 和 Windows 的 AD，移动 APP、移动 VPN、以及移动工作空间等需要设计合理的认证时序，并通过 SDK 集成的方式，实现与已有 IAM 平台的集成，使用 IAM 平台完成集中身份管理和认证服务，并且在多应用之间通过 Token 传递实现单点登录。

为了简化移动应用的用户身份管理和身份认证，陆续出现了一些比较有影响力的与身份协议栈有关的互操作协议，而且随着应用实践的发展，持续发布成熟度更高的协议版本，目前具备较多使用场景的包括 OIDC、OAuth2、FIDO2 等，其中 OIDC 和 Oauth2 可以实现多个应用使用单个应用的用户身份完成用户登录，FIDO2 则能够依托本地可信执行环境 TEE，利用非对称密码技术和生物特征识别技术，实现免密码的强身份认证，彻底杜绝认证服务端大量存储的用户名/密码数

据被拖库造成泄露的风险。

(4) 用户认证与设备认证的结合

在移动办公和移动业务应用场景中，仅仅在应用上认证用户身份是不够的，更安全的方式是将用户认证和设备认证结合起来进行身份认证，移动端安全软件会收集移动端设备信息，通过计算生产设备指纹，在移动端请求访问时，在服务端完成设备指纹是否与注册指纹匹配一致，只有当用户认证和设备认证均通过的条件下，移动应用 APP 才能够与服务端进行业务操作。

2. 数据安全传输

(1) 安全传输协议

在移动办公和移动业务应用场景中，移动端到服务端之间的数据传输所使用的安全传输协议，与 PC 互联网相同，仍然是使用 SSL/TLS 等安全协议，完成双向的强身份认证，在认证基础上完成会话密钥协商，使用会话密钥对通信内容进行加解密和完整性保护，具体的实现方式分为两种:

- 使用传统的 SSL VPN 网关设备和移动端 VPN 客户端，这种使用方式往往是出于对已有的 SSL VPN 网关设备的利旧使用考虑，对于移动端来说，这是一种设备级 VPN 通道，而非应用级 VPN 通道，所有的移动业务 APP

都会使用相同的 VPN 通道完成数据传输，而且往往移动端用户操作要分为 VPN 登录和应用 APP 登录两个步骤，可能带来不好的用户体验;

- 使用移动安全接入网关，移动端的 VPN 客户端模块集成到为移动应用 APP 提供安全保护的应用级容器中，每个受保护的移动应用 APP 单独与移动安全接入网关之间完成身份认证、秘钥协商和安全通道建立，这是一种更高级形态的应用级 VPN 通道，而且可以实现 VPN 通道建立过程对移动端用户透明，从而带来更便捷的用户体验。

(2) 国密算法

有些对数据安全性要求较高的移动业务场景，可能对数据安全传输和存储要求使用国密算法，即国家密码管理局认可的国产密码算法。负责完成 VPN 通道建立的客户端和服务端组件的协议实现，除了支持 RSA、AES、SHA1 等国际标准密码算法之外，还需要支持下列国密算法:

- SM2 非对称加密，基于 ECC 椭圆曲线。该算法已公开，该算法秘钥长度 256 位，安全强度比 RSA 2048 位高，且运算速度快于 RSA。该算法用于安全通道握手过程中的双向身份认证和数字签名;

- SM3 消息摘要算法，该算法已公开，校验结果为 256 位。该算法用于对通信内容进行完整性校验；
- SM4 对称加密算法，密钥长度和分组长度均为 128 位。该算法用于对通信内容进行加密保护。

(3) 密钥管理

移动端可能在操作系统层面被恶意代码感染或者非法控制，攻击者可能会在掌控移动端运行环境情况下实施针对加密算法的白盒攻击，例如分析内存内容，从中提取出加密密钥，进而解开受保护的数据而造成泄密；或者对移动 APP 进行逆向后，进行跟踪调试，从内存中提取出加密密钥。传统的软件开发，无论是在代码中写入密钥还是调用函数产生密钥，都无法应对白盒攻击带来的威胁。

要对抗白盒攻击威胁，需要将密码算法和密钥通过混淆技术实现白盒化处理，不让密钥出现在运行环境中，提高攻击者获得密钥的难度，从而确保受加密保护数据的机密性，目前针对 AES 国际标准算法和 SM4 国密算法，均已有较为成熟的密钥白盒实现。

密钥白盒技术分为以下两类：

- 静态密钥白盒，是将密钥和加密算法绑定混淆，生成密钥白盒，一个密钥对应一个密钥白盒，以库文件形

式存在，需要在开发应用程序时集成到工程里。这种实现方式提供了一个受保护的固定对称密钥白盒，可用于数据传输和存储，但会面临密钥更新的难点；

- 动态密钥白盒，以白盒库的形式为应用提供可动态变化的密钥白盒，进一步提升分析出原始密钥的难度，可用于对数据安全性要求很高的移动业务场景。

3. 移动端应用级安全容器

容器是为执行中的程序提供隔离环境的一种安全机制。它通过严格控制执行的程序所访问的资源，以确保系统的安全。应用级容器技术是一种在移动操作系统底层实现的、提供移动应用 APP 安全保护能力的技术，在无需获取应用源代码，也不需要 Root 权限、在代码零改造的基础上对应用形成一个有隔离保护的移动 APP 安全运行环境，在该安全环境中可实现各种移动业务安全运行的通用性需求，例如：数据防泄露、应用功能安全调用、运行安全保护和隐私类保护等，也可快速的适配实现企业其他个性化的网络安全保护和内容审计及其他需求。

默认情况下应用 APP 可以访问和请求任意的系统资源，比如读取，删除一些文件或者网络操作等，但通过应用级容器实现建立一个单独的、安全的虚拟系统，构建在应用和系

统之间，从系统底层对应用权限和用户使用行为等进行全方位的管理和保护，应用发起的请求先经过应用级安全容器进行安全判断和审计，阻断不安全请求，防止将应用中的敏感信息外泄等情况，使企业应用运行在一个安全可靠的环境中。

在开放的安卓系统中，应用级安全容器可以有不同的实现方式，而且能够提供较为细化的安全管控能力，不同的技术实现在安全能力集合、封装效率、应用适配、使用稳定性等方面会存在差异。在封闭的 IOS 系统中，应用级安全容器的实现较为困难，且能提供的安全控制能力也会明显少于安卓系统的容器。

图 13 应用级安全容器原理

应用级安全容器技术提供两种方式对移动应用 APP 进行安全赋能：

(1) Wrapping 集成

将 APP 上传至移动安全管理平台，通过独立的 Wrapping

服务器将应用级安全容器 SDK 打包至 APP 中，得到封装之后的 APP，并发布使用。

(2) SDK 集成

使用 SDK 方式集成时，移动应用 APP 开发方需在开发过程中集成应用级安全容器 SDK，作为受保护的 APP 进行发布和使用。

4. 移动端防敏感信息泄露

数据泄露防护（Data leakage prevention，DLP），又称为“数据丢失防护”（Data Loss prevention，DLP），是通过一定的技术手段，用来防止指定数据或信息资产以违反安全策略规定的形式流出，是目前国际上主流的信息安全和数据防护手段之一。

不同于传统 PC 端的数据泄露防护，移动端由于设备、网络、应用、操作系统、传输链路等各种复杂因素交织在一起，往往比 PC 端数据泄露途径更广，防护要求技术点更琐碎。

从移动应用层面，数据泄露途径通常包括:

- 操作泄露：通过截屏、录屏、复制、粘贴、下载等操作泄露数据;
- 共享泄露：通过调用社交工具、邮件系统客户端发送

数据;

- 通过蓝牙、WiFi、打印等技术实现数据共享;
- 恶意程序窃取，木马或恶意程序对移动应用数据进行窃取等。

(1) 移动应用数据泄露防护（DLP）实现原理

可以通过对移动应用改造来实现应用数据泄露防护，通常使用应用级安全容器技术对移动应用进行 DLP 防护。首先通过封装让移动应用运行在安全容器内，再根据不同业务场景对应用安全策略的需求，通过安全容器管理后台配置不同的 DLP 策略，并下发给该应用的安全容器。

受到安全容器保护的应用在向操作系统进行操作（复制、截屏、转发、打印、下载、使用其他应用打开等）申请时，需要通过容器进行判断这些操作是否违反 DLP 策略规定，违反的会自动拦截，无法传递给操作系统进行执行，符合规定的会自动放行。

当移动应用的 DLP 策略规定发生变化时，可以通过管理后台进行调整，并同步给安全容器进行执行。

(2) 移动应用数据泄露防护（DLP）策略

根据移动办公和和移动业务应用场景对数据泄露防护的需求，DLP 策略主要集中在应用的分享控制、数据加密、

水印、应用调用控制、应用功能调用限制、应用网络保护等方面。

由于应用安全容器技术实现路线的不同，存在着稳定性、应用适配性、封装效率方面的差异，在开源的安卓系统上安全容器所能够实现的 DLP 能力，会明显优于封闭的苹果 IOS 系统上安全容器所能实现的能力。以安卓操作系统为例，可以进行配置的策略主要包括：

表 6 安卓移动端防敏感信息泄露策略

应用分享控制	应用加密	应用水印	应用调用控制	其他功能调用控制	应用网络保护	应用无痕使用
禁止应用复制粘贴	应用数据加密	明水印	禁止调用系统应用	禁止应用调用短信	禁止应用使用 WIFI	应用退出清除数据
禁止对应用截屏	应用文档加密	暗水印	禁止调用第三方非安全应用	禁止应用调用摄像头拍照、摄像	禁止应用使用移动网络	应用进程关闭清除数据
禁止对应用录屏			禁止调用安全应用	禁止应用使用蓝牙传输		
			禁止调用邮件客户端发邮件	禁止应用使用录音		
				禁止应用获取地理位置		
				禁止应用使用打印		
				禁止应用访问多媒体资源		

随着移动业务场景的不断深化，及应用级安全容器技术

的不断发展，DLP 策略会更加贴合业务场景，并为业务场景服务。

5. 移动 APP 加固

移动应用加固主要从技术层面对移动 APP 的 DEX 文件、SO 文件、资源文件等进行保护。移动应用加固是 APP 安全的重要防护手段，利用移动应用加固可在一定程度上保护 APP 的核心代码算法，提高逆向破解、二次打包的难度，有效缓解恶意攻击。

没有保护的 APP 会面临多重风险，如:

- 界面劫持: 恶意程序监听应用程序的界面对敏感界面进行劫持替换，获取用户敏感信息;
- 二次打包: APP 发布后，通过反编译的方式在客户端程序中植入木马或其他恶意代码，并通过诱骗分发，以窃取用户的隐私信息或植入广告等;
- 证书弱校验: APP 缺乏对 SSL 证书的校验，导致 TLS 中间人攻击;
- 组件暴露: Android 四大组件属性 Android:exported 为 true 导致组件可被绕过，本地拒绝服务等风险。

为有效应对以上威胁,执行移动 APP 脆弱性检测和加固，以及后续应用发布渠道监控等机制，能够有效减轻以上问题。

(1) 在移动应用上线前，企业应执行应用检测，包括并不限于，本地数据存储的安全检测和评估，APP 数据安全传输检测和评估，APP 认证和鉴权的安全机制的检测和评估，数据安全上传的检测和评估，终端 APR web 应用安全检测和评估，终端完整性的检测和评估等，对各种应用漏洞，恶意代码等进行分析。同时也可以通过渗透测试的方式来模拟黑客攻击，以验证漏洞并评估对具体业务风险的等级。

(2) 应用加固有多种策略，如：

图 14 移动应用加固策略

为应对不断出现的新型黑客攻击手段，加固技术也经历了包括代码混淆保护技术、Dex 文件整体加密保护技术、Dex

函数抽取加密保护技术、混合加密保护技术、虚拟机保护技术等技术的演进和更新。

- 代码混淆保护技术：主要是对 Java 字节码进行混淆，比较常见的代码混淆有 proguard 和 dexguard,其中包括了名称混淆、字符串加密、反射替换、日志清除、花指令等;
- Dex 文件整体加密保护技术：DEX 文件整体加固保护技术是基于类加载的方式来实现的，整个加壳的过程涉及到三个程序：源程序，加壳程序，解壳程序。基本原理是对 Dex 文件进行整体加密后存放在 APK 的资源中，运行时将加密后的 Dex 文件在内存中解密，并让 Dalvik 虚拟机动态加载执行;
- Dex 函数抽取加密保护技术:对代码中的每个方法抽出并进行单独加密，利用 Java 虚拟机执行方法的机制来实现。利用这个机制将解密操作延迟到某个方法在执行之前才开始加载该方法的代码，同时解密后的代码在内存是不连续存放的;
- 混合加密保护技术：混淆加密可以隐藏 dex 文件中关键的代码，力度从轻到重包括：静态变量的隐藏、函数的重复定义、函数的隐藏、以及整个类的隐藏。混

淆后的 dex 文件依旧可以通过 dex2jar jade 等工具的反编译成 Java 源码，但是里面关键的代码已经无法看到；

- 虚拟机保护技术：虚拟机软件保护技术应用层级不同，基本可分为硬件抽象层虚拟机、操作系统层虚拟机和软件应用层虚拟机。用于保护软件安全的虚拟机属于软件应用层虚拟机，是对被保护的目标程序的核心代码二进制文件进行“编译”，将由编译器生成的本机代码（Native code）转换成效果等价的 byte-code，然后为软件添加虚拟机解释引擎。用户最终使用软件时，虚拟机解释引擎会读取 byte-code，并进行解释执行。

(3) 应用上线发布后，企业应监控应用的发布渠道和下载网站，监测其中出现的盗版、破解、钓鱼、仿冒等情况。对安全性要求较高的企业，应建立企业独立的应用商店，以防止应用被恶意攻击。

六、发展趋势预测

（一）移动应用场景快速丰富

移动通信基础设施的技术发展将进一步推进移动互联

网的发展，5G 网络投入商用必然将带来新的变革，5G 移动通信技术所具备的高带宽、低时延、高密度接入的优异特性，将能够更好地支持现有移动办公和应用的运行，提升用户体验。另外，还会有很多行业关键业务应用，在 5G 条件下具备了实现移动化的可能，成为可能获得巨大发展的新兴移动业务场景，例如车联网、医联网、工业互联网、以及其它形式的泛在物联网。

赛迪智库和通信产业报、华为、中国信息通信研究院等媒体、厂商、研究机构都在 2019 年发布了 5G 创新应用场景的研究和趋势预测报告，结合当前 5G 应用的实际情况和未来发展趋势，预测了 VR/AR、超高清视频、车联网、联网无人机、远程医疗、智慧电力、智能工厂、智能安防、个人 AI 助理以及智慧园区等多个创新应用场景，还预测了各个场景的融合应用时间进度。

图 15 5G 领域专业报告

（二）BYOD 自携设备成为主流模式

根据 Gartner 的调查，在 2017 年 BYOD 的普及率就已经达到并超过了 50%。调查机构 ForresterResearch 的调查数据显示，约 70%的被调查企业会考虑采取 BYOD 的移动办公计划。

BYOD 设备已经从 PC 电脑为主，发展为以智能手机/智能平板为主，BYOD 使用模式下，用户的需求集中于如何在一台设备上隔离出私人生活空间和工作空间，以及如何平衡好对移动办公数据的安全风险管控与员工个人隐私信息保护之间的关系，设备级管控方案可能会侵犯个人隐私而越来越显得灵活性不足。

BYOD 个人自携设备场景将进一步成为主流趋势，移动设备形式将以更加通用的智能终端设备为主，移动安全的关注领域也将继续从最初的移动设备管控向移动应用管控转移，未来的移动安全将呈现以移动应用为中心，与移动应用相融合的趋势。

（三）移动应用服务面临安全威胁水平提升

移动办公和业务应用，需要通过开放的移动互联网提供服务，开放网络中的恶意代码、入侵攻击、拒绝服务攻击、钓鱼欺诈等安全威胁水平本身就较为严重，近年来，大规模

的数据泄露、以及侵犯个人隐私等事件层出不穷，频繁曝光的高危级别安全漏洞更说明了各类关键信息基础设施在面对安全威胁时自身防御能力的不足。

当越来越多的办公和业务场景实现移动化之后，由于重点行业机构的移动办公和业务应用所处理的信息敏感性和数据价值更高，必将吸引更多的恶意攻击者的注意，从而带来更高的外部安全威胁，从而提升移动办公和业务系统运行的安全风险级别。

各行业机构应当清楚认知业务移动化所面临的安全风险严峻局面，必须有意识将业务移动化建设与安全风险管控同步考虑、同步设计、同步实施，确保移动办公和业务系统具备适当的安全风险控制能力。

（四）移动办公与业务系统面临更强的安全合规监管

国家网络安全监管政策将进一步提升对移动安全领域的重视，并催发更多的安全保障建设需求，等级保护 2.0 标准的变化的具体体现，就是使得更多移动办公和业务应用，需要满足对应等级的安全通用要求和安全扩展要求，等级保护 2.0 标准已于 2019 年 12 月正式实施，将使得更多的行业用户越来越关注移动互联场景下的移动应用安全保障合规。

另外，国家层面的安全监管越来越重视对个人信息的保

护，国家市场监督管理总局、国家标准化管理委员会发布的GB/T 35273-2020《信息安全技术 个人信息安全规范》，信安标委发布的《移动互联网应用基本业务功能必要信息规范》，四部委联合发布的《App 违法违规收集使用个人信息行为认定方法》，以及四部委主导执行的关于移动 APP 过度索权、侵犯用户个人隐私的检测和处罚专项治理行动，都使得移动办公和业务应用需要严肃对待用户隐私保护的问题。

（五）平台级解决方案更具竞争力

随着业务移动化进程的推进，行业机构的移动业务场景也日趋复杂，往往既存在配发设备移动业务场景，也存在自携设备移动办公场景，既要对一部分场景进行移动设备管控，又要对一部分场景进行移动应用和数据管控，可能存在数量较多的原生业务应用和 H5 轻应用，不同的移动业务场景对安全管控的能力也存在差异化的需求。

市场将更加需要能够适应移动业务场景的尊重用户体验和快速迭代交付传统，并能够为移动业务场景提供综合安全赋能的平台级解决方案，一次性建设后，为多个移动业务场景提供统一、灵活的安全管控能力，逐渐取代针对单个移动应用进行加固赋能的模式，平台级解决方案在市场竞争中将具备更强的竞争力，得到市场中头部客户的青睐。

附录 A 典型企业移动办公应用安全保障案例

（一）指掌易移动业务智能安全平台（MBS）

指掌易移动业务智能安全平台（MBS），秉承“安全业务化、业务安全化”的安全理念，在不影响原有业务的基础上为企业移动办公业务提供云、管、端全方位的安全赋能。在移动终端上为企业员工提供一个独立的安全工作空间，将企业移动业务运行在安全工作空间内，与个人区域完全隔离，保护企业数据在移动设备上的安全；在传输端，建立应用级安全传输通道，保障企业数据在传输过程中的安全；在服务接入侧，建立安全接入网关，对接入的用户、应用、设备进行多维度的安全评估与认证，确保服务接入安全。

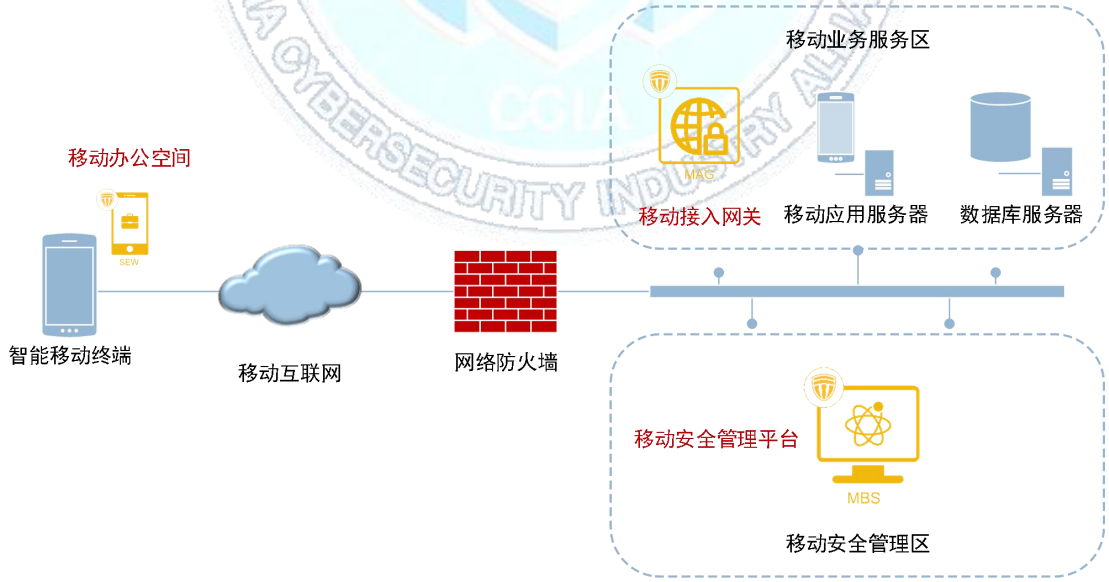

图 16 MBS 移动业务安全解决方案构成

移动业务智能安全平台为企业打造全链路、集约化、可扩

展的移动安全平台，基于底层各类安全能力赋能上层各类办公业务。

图 17 MBS 移动业务智能安全平台架构

➢ 应用安全

移动应用是企业移动办公业务的主要载体，针对移动应用的安全防护，指掌易提供了基于安全工作空间的应用全生命周期的安全能力支持。

应用漏洞扫描与加固：针对移动应用包，在员工使用之前，对应用包进行安全漏洞扫描与加固，防止第三方对应用包恶意篡改、逆向、恶意调试;

应用安全入口及应用市场：针对企业移动业务应用的使用与管理，提供统一的安全工作空间，将企业各类移动应用运行在安全工作空间内，实现安全防护。同时提供统一的应用市场，供企业统一发布、统一使用移动业务;

移动威胁感知（MTD）：移动威胁感知（Mobile Treat

Defense），提供在安全工作空间边界范围内的安全威胁检测与防御，从设备、应用、网络等角度进行全面合规检查，确保安全工作空间范围内的环境安全;

双因素认证: 平台提供了短信验证码、指纹、人脸、图形等附加认证机制，可配合应用原有的账号密码认证，实现双因素认证模型。增强应用认证安全性;

数据落地隔离与加密: 移动化办公业务普遍具有本地缓存、文件下载的能力，对于产生在移动设备本地的数据缓存或文件，提供透明加解密能力，加强落地数据安全防护能力;

应用数据防泄漏: 针对移动应用提供数据防泄漏能力，防止应用层数据外泄，包括屏幕水印、防截屏、防复制黏贴、防分享、防打印等

- **设备安全**

针对具有派发移动设备的场景，对派发的移动设备进行设备级安全管控。

资产管理: 对企业采购的移动设备提供了设备资产录入、过程管理、设备淘汰全流程管理;

设备管理: 对设备的静态、动态信息均进行了详细的记录与动态更新与管理;

策略管理: 针对移动设备可设定不同业务场景下的安全策

略，并支持针对不同人员设定不同安全策略;

违规检测：针对设备、应用、及策略维度设立合规策略，只有在完全合规的环境场景下，用户才能合法使用移动设备及移动业务，若产生违规情况，可根据设定的合规策略执行相应的安全措施;

远程管理：针对已录入资产库在正常使用的设备，管理员可进行远程安全管理，包括远程策略管理、远程安全管理等。

- **传输安全**

通过指掌易移动安全网关产品模块(MAG),将企业的业务服务器隐藏在企业内网，通过安全网关进行数据转发，同时安全网关与移动设备之间建立安全传输通道，实现传输安全。

SSL 协议加密传输：安全隧道采用了 SSL/TLS 协议（RFC2246），加密算法支持 AES256、国密 SM4，确保所有数据在一个安全、可信的信道中传输，防止传输过程中被非法窃取、篡改等风险，从而保障企业数据传输通道的安全性;

SSL 双向认证保护:用户端与 MAG 建立安全通道，除了普通的用户名密码或者短信认证外，还会做双向的证书认证。需要客户端与服务端证书认证通过后才能建立安全隧道，增强了用户身份认证的安全性;

国密算法支持:支持国际通用的商用密码算法 AES256，同

时也支持国家密码管理局规定的国产商用密码标准 SM4,保障用户的业务安全传输;

应用级安全隧道: 应用自动封装即可具备安全接入能力。业务应用只需关注其业务能力，不需要在应用集成联调方案层面重复投入，降低技术难度。针对不同的 APP 应用建立不同的安全隧道，实现信道传输的微隔离。

- **认证安全**

统一用户及认证: 提供移动应用身份管理服务，后端与企业 AD/LDAP 等用户系统对接，前端为各类移动应用提供统一身份认证管理，实现移动业务单点登录(SSO)，即以移动安全空间/门户为中心，一次登录，关联应用即可免登录;

组合认证模型: 鉴于单独账号密码认证具有被攻击的风险，平台将用户、应用、设备统一进行身份化，在用户接入认证时同时对用户账号、应用、设备进行组合认证，仅在组合认证通过时才允许接入。

- **安全办公套件**

平台提供日常办公中常用的安全办公套件，基于安全和用户体验满足员工各类办公需求。包括安全邮件、安全通讯录、安全云盘、安全相机、安全浏览器等。

（二）中国移动保障移动办公业务安全解决方案

为抗击新型冠状病毒，助力政企行业复工复产，中国移动推出一系列移动办公解决方案，并组织全集团网信安全专家采用“深度体检+智能风控”等手段，对相关业务进行全方位检测、全天候护航、全时段保障，确保业务安全平稳运行。在抗击新型冠状病毒的前两个月内，已为 25 个重点业务排查内生安全风险 32 项，拦截黑产攻击 2 亿次，积累攻击源环境、攻击设备、攻击账号等黑产特征 1287 万个。针对邮箱业务账号撞库攻击典型风险，通过知识图谱和图计算复杂网络模型的离线分析，成功定位到了横跨数省掌控上万 IP 的某黑产团伙。

方案包含风险评估和风险监测两部分，如图 18 所示。

图 18 中国移动保障移动办公业务安全工作模式

- **重点风险评估**

中国移动安全专家团队在《中国移动业务安全通用评估规范》的基础上，针对抗疫背景和政企办公业务特点，建立了覆盖 7 大类 30 余项的重点安全风险排查矩阵，坚持 7x24 小时不间断“云复盘”、“地毯式体检”，有效排查政企移动办公业务在特殊时期面临的黑产定向攻击、钓鱼木马等重点安全风险。

- **智能风险监测**

针对移动办公业务在抗疫期间频繁遭受黑产定向攻击等挑战，中国移动创新研发上线了业务风险控制监测系统，实现及时、精准、全面的业务风险感知和防护处置。该系统基于行为识别和智能模型，集合安全行为分析策略，具备多维度数据综合分析能力，可智能识别、研判与拦截业务风险，并追溯黑产攻击犯罪链条。

中国移动业务风险控制监测解决方案主要包括 7 大模块，如图 19 所示:

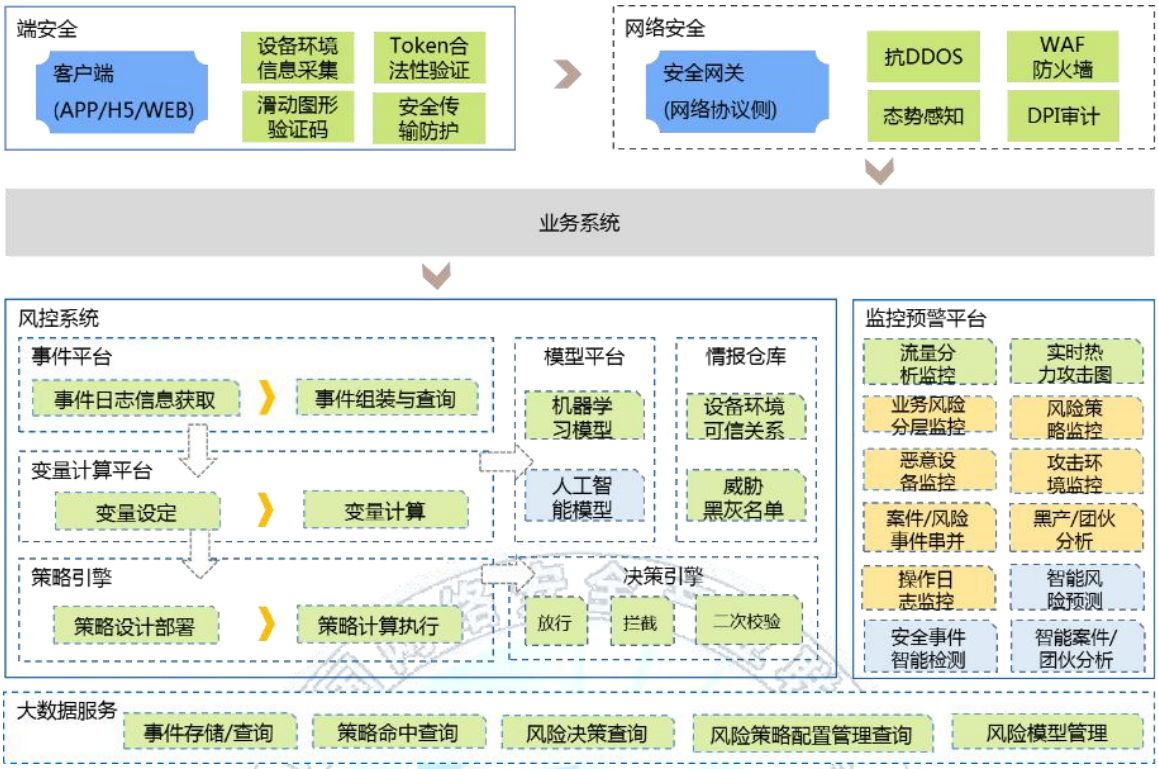

图 19 中国移动业务风险控制监测解决方案

- **事件平台**

风控事件包含设备信息、环境信息、业务属性等用户操作请求信息，是业务风控的处理对象。

- **变量计算平台**

用于累积历史上用户行为链数据，实时计算变量供策略引擎实时调用，亦可供模型训练和模型平台模型部署使用。

- **策略引擎**

基于海量风险行为分析策略，实时识别业务风险范围。具有高并发、毫秒级低延时、智能非线性并发、高可扩展性等特点。

- **模型平台**

为风险识别模型实时计算提供承载平台，使用机器学习（如逻辑回归、随机森林、GBDT 等）和 AI 深度学习模型（如 DBN、CNN、RNN、DNN 等）应用于业务风险识别。

- **情报仓库**

包含各类风险情报大数据信息，包括可信关系信息库，黑白灰名单信息库等。

- **决策引擎**

实现多策略模型识别命中后的合并处理，实现风险实时智能化归并，给业务输出智能化统一管理的适合的管控手段。通过风险智能决策管控，完成对攻击的实时拦截和告警，实现用户无感知、业务不停歇、风险实时管。

- **监控预警平台**

可视化展现业务流量波动、实时攻击热力地图、黑产团伙串并联分析、业务风险监控预警、恶意设备/攻击环境监控等功能。

图 20 中国移动业务风险实时监控大屏

（三）安天智信零信任移动应用安全交付系统（zADS）

安天智信零信任移动应用安全交付系统（zADS）是在零信任安全架构基础之上，为企业建立一套完整的虚拟安全边界并提供更加安全的应用访问环境。通过统一身份认证、单点登录和链路透明加解密为企业提供应用安全访问入口，比传统 VPN 更安全更便捷；通过 web 应用移动化和终端环境检测为企业提供低成本的安全移动办公环境；通过身份、状态、行为、内容的零信任策略，为企业提供动态访问控制，以此保障应用访问安全性；通过数字水印、文档不落地、邮件代理，为企业数据资产全生命周期保驾护航。

安天智信零信任移动应用安全交付系统由智信安全工作空间（SDK）、智信应用安全交付网关、零信任策略优化平台组成。通过智信安全工作空间或 SDK 保障终端安全，通过智信应用安全交付网关保障企业内部应用服务的访问安全，通过零信任策略优化平台提供应用访问控制策略的动态计算能力，同时结合安全移动威胁情报能力，进一步增强应用访问的异常判定及访问控制策略的动态调整，从而全方位的保障应用访问的整体安全性，实现应用访问全生命周期安全的可靠、可控、可视、可查。架构图如图 21 所示。

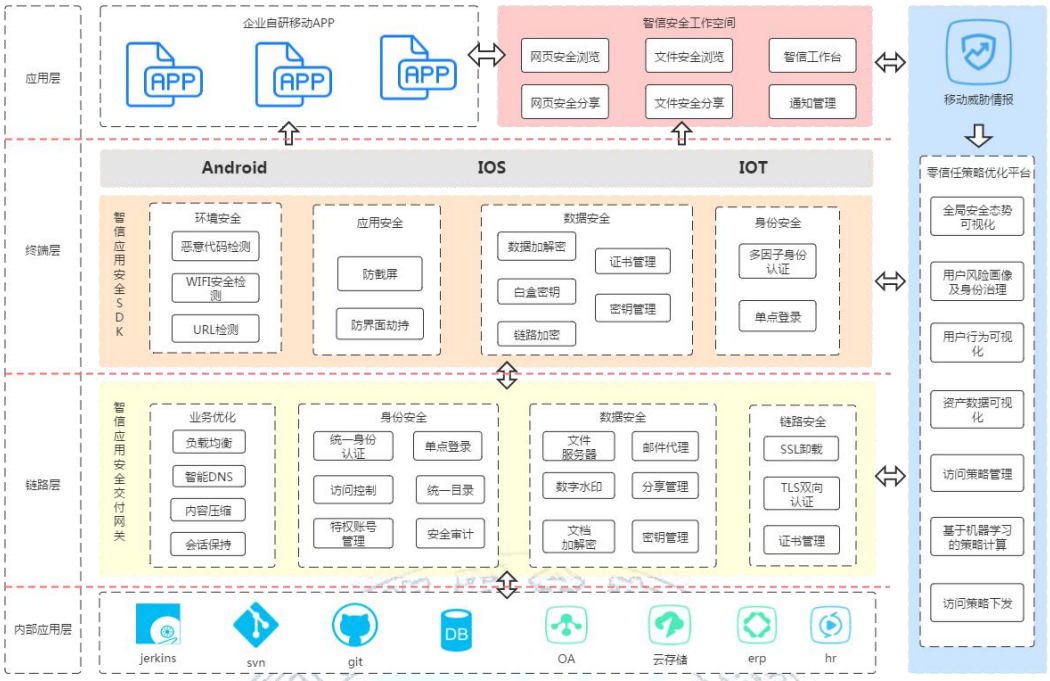

图 21 安天智信零信任应用安全交付系统产品架构

以安天智信零信任应用安全交付为基础，结合安天终端安全防护、内网安全监测、远程应急响应和定制可视化指挥舱等产品能力优势，为政企移动办公业务场景的接入使用、安全管理、安全监测、安全处置、安全决策提供全方位安全能力和综合方案保障支撑。方案如图所示。

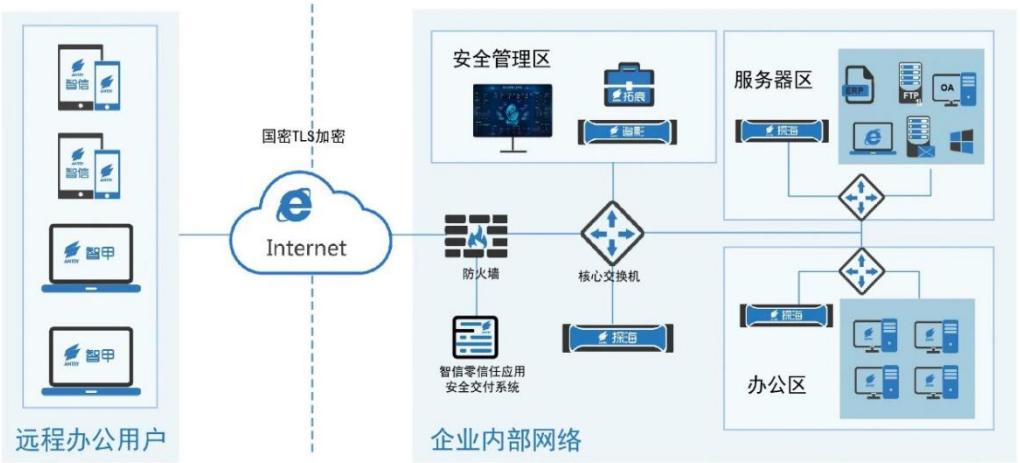

图 22 综合安全保障方案

➢ 为企业内网及业务系统提供统一身份认证、多因子认证、单点登录和链路透明加解密等措施，保障应用访问入口安全。支持二维码扫码认证、图形码认证、LDAP 认证、互联网认证（QQ/微信/企业微信认证）、双因素认证（OTP/PKI/短信验证码）、生物特征认证（基于 IFAA 指纹认证）等多因子身份认证方式。支持国密 SM2/SM3/SM4 系列算法，RSA/ECDSA/SM2 类型证书，prime256v1/secp384r1/sm2 ECC 椭圆曲线。

➢ 为企业安全管理者提供基于身份、状态、行为、内容的零信任策略手段，构建应用访问控制策略的动态管控能力。提供员工行为画像、信誉评估等整体安全态势，按需打造可视化指挥舱支撑企业安全决策。

➢ 敏感文档检测能力。支持对邮件附件、文件分享、文件下载进行安全防泄密审查，通过对涉密文档生成 MD5 和敏感关键字配置，发送邮件、文件分享下载时对文档进行 MD5 匹配和敏感关键字匹配，配合数据防泄漏管理策略，通过附件加水印、附件公钥加密、阻断外发，防止文件被泄密。

➢ 多场景动态策略管控。基于零信任安全架构，提供基于用户身份、行为、内容、环境的动态安全访问控制策略。策略优化平台内置身份、终端、邮件、文件、行为、关系、

需求、属性 8 大场景策略，50+安全策略模型，基于用户身份、行为、状态智能计算安全策略。基于动态策略模型动态调整应用访问控制策略，保障企业应用访问安全，使员工可随时随地安全的访问企业应用。

- 多端协同保障数据安全。覆盖“访问、交互、传输、存储”立体化数据安全防护，基于国密算法的链路加密，拥有终端防截屏、防复制粘贴、基于身份的透明水印、文档不落地浏览等功能；以及终端手机数据加密，关键数据使用白盒密钥加密，服务端数据存储加密等功能。
- 灵活交付快捷上线。灵活的交付模式适合不同的部署场景，不影响现有网络结构，支持多种认证方式，无改造单点登录，一键生成移动端应用，PC 环境良好适配低占用。

（四）蓝盾企业移动信息化安全管理系统（S-EMM）

蓝盾企业移动信息化安全管理系统（S-EMM）是企业移动业务终端场景化安全解决方案，通过对设备的系统策略管理、对应用的安全加固防护、对服务的全流程加密，使业务单位能够轻松应对差旅办公、家庭办公、企业级无线接入、移动执法、户外勘测等各类应用场景的安全问题。

产品集成 MDM、MAM、MCM、MI、Containment 模块，能够从终端的配置、应用、内容、网络等多个维度进行全方位

安全防护。该方案将给移动化办公带来全新的模式。

蓝盾 S-EMM 具有非常灵活的部署模式，可以在完全不改变网络架构、网络设备配置的情况下轻松部署到信息系统中。产品采用高可靠工控机硬件设备，服务端软硬一体化并通过网络协议与客户端进行连接，有效的管理企业内部无线接入设备与外部移动办公终端。

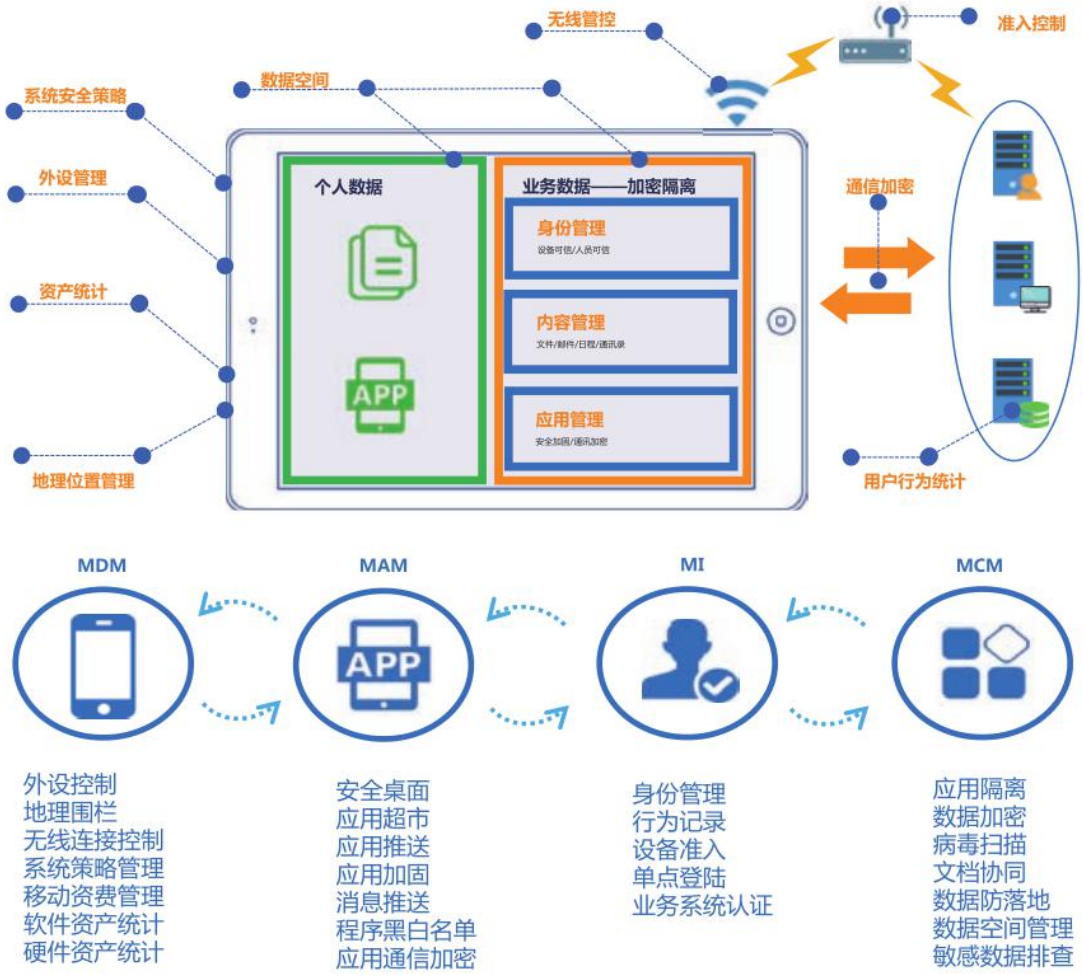

图 23 产品架构

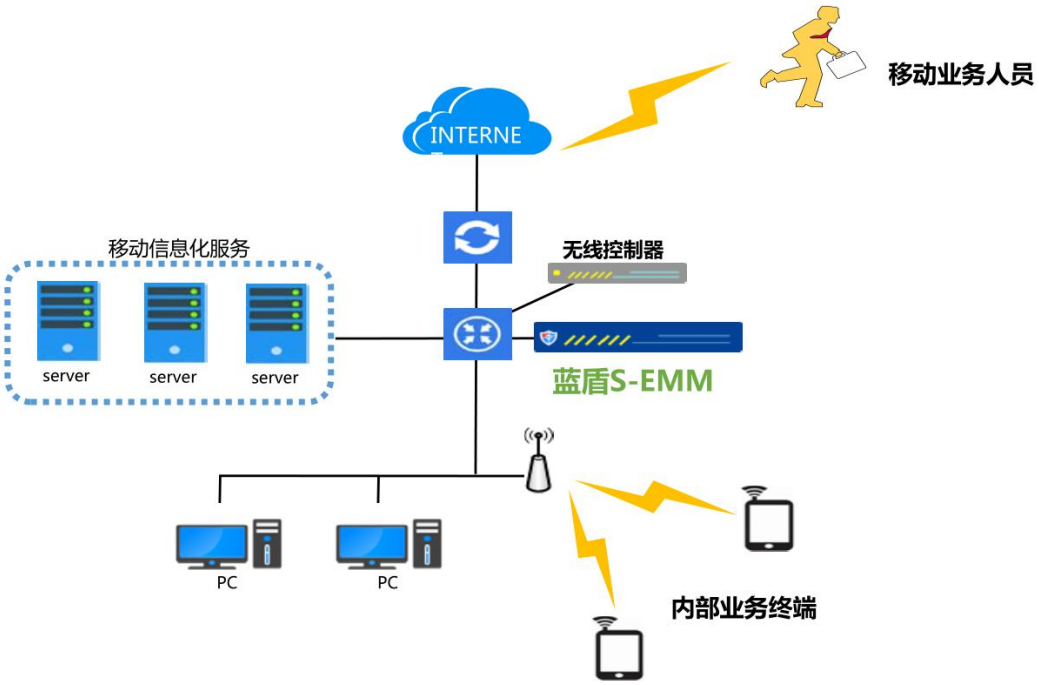

图 24 系统部署

- **独特的防病毒管理**

集成蓝盾安全卫士杀毒软件，不仅能实现安全管理策略，而且能够有效查搜移动设备中的各类蠕虫、木马等病毒软件，对业务环境从底层代码到办公流程实现全方位安全管控。

- **全面的无线设备联动认证**

可以采用标准认证协议与企业级无线系统进行联动准入控制，将非法设备彻底隔离在网络之外，确保移动信息化系统终端与服务均不受不可控因素的影响。

- **一键式应用加固**

将应用安装包上传至服务端即可自动进行应用加固，简单易用。

- **用户行为分析**

支持强制终端受控接入、实名接入。受控接入确保终端安装客户端才能入网，具有审计登录地点、访问应用、执行操作等行为的功能；实名接入则确保所有行为的审计能够责任到人。

两者结合可以实现全面的用户行为分析，对用户的异常登录、不安全访问、威胁行为等安全问题进行全面预警与防护。

（五）绿盟科技零信任安全解决方案

绿盟科技遵循体系化的安全框架，围绕零信任理念，在终端安全，身份识别与管理，网络安全，应用和数据安全，安全分析协作与响应等多个方面，为客户提供完整的可落地的零信任安全解决方案。

零信任网络默认不信任任何设备和用户，用户和设备经过验证后，持续监控设备安全状态和用户行为，一旦信用等级下降，动态调整访问级别，有必要还会切断访问会话。

零信任是一种主动的安全模型，基于设备评估和用户认证，并集成持续分析和验证信任关系，以此确保网络上的实体没有恶意行为，从而降低和消除安全风险。

- 连接之前先认证

任何设备和用户，在访问应用前先取得认证和授权才能访问资源。这种方式和防火墙访问控制有着很大不同。防火墙访问控制规则，资源（应用或者服务）是开放的，用户先访问资源，然后根据系统需要来认证和授权。此外，基于位置和 IP 地址的访问控制策略，不足以确认访问实体是否合法（比如被入侵的客户端）。

- 基于访问语境的访问

零信任网络不是简单地依赖于“用户名/密码”来控制访问。理想的模型，包含多个属性的评估。设备的身份属性，用户身份，设备当前安全性（比如重要补丁，关键注册表项，用户，程序，当前进程等），这些访问相关的上下文语境，构成了信任的元素。只有超过预设的信任等级，才能被授予访问权限。

- 持续评估信任关系

访问初始的信任，不是一次性的，需要持续地评估。这得益于 UEBA（用户和实体行为分析）技术的发展，持续对接入设备的行为分析，确保没有恶意行为发生。一旦发现访问实体的异常行为，比如扫描或者暴力破解，意味着信任等级的降低，零信任网络可以切断这种访问，从而降低安全风险。

- 最小权限

最小权限意味着设备或用户获得完成任务的最小权限。微

隔离（Micro-Segmentation）技术，根据服务和区域，将网络切片隔离，避免攻击的横向扩展，常常应用在零信任网络中。

可以看出，零信任并未引入新的技术。而且很多技术（比如认证、授权、设备安全，包括 UEBA）企业或多或少都有部署。然而，将这些技术重新排列组合，却是新颖的方式。

图 25 零信任安全解决方案架构

➢ 安全接入网关

安全接入网关，以反向代理方式，对外发布应用资源。安全接入网关将外网用户和内网资源隔离，过滤非法的访问。此外，安全接入网关，为内部应用资源提供加密访问通道，与设备之间通过证书来认证，增强安全性。

➢ 统一身份认证平台

统一身份平台，集合了用户、认证、授权、应用、审计的统一管理功能，是用户身份和访问管理的平台。用户管理，将各子系统的账户关联到主账户中，实现账号体系的统一，方便

员工的生命周期管理。 统一身份平台可以利用第三方账户数据，周期同步。

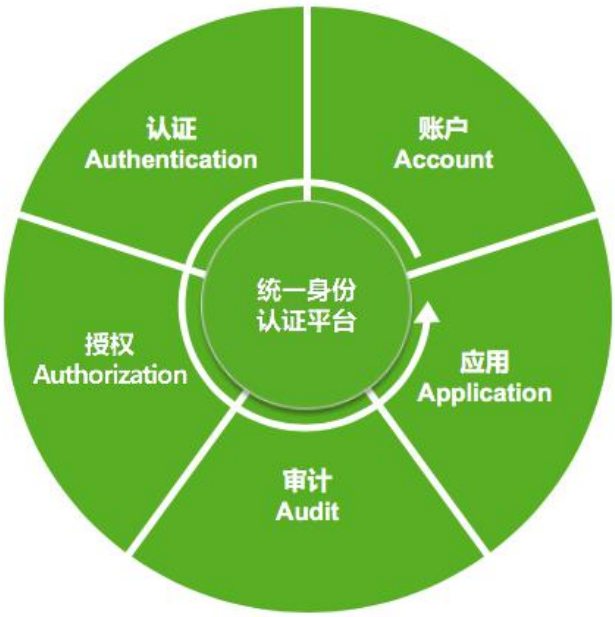

图 26 统一身份认证平台功能

单点登录（SSO），采集多种认证因子，通过票据（Token）到不同应用的服务端进行认证，实现统一认证和单点登录 。

多因素认证（MFA），与移动设备相结合，可以实现多因素认证。比如一次性认证码（OTP），短信认证，Mobile Push 等方式认证。

- 策略引擎平台

策略引擎平台，设置信任评估的策略，下发访问控制策略。信任评估的要素，来自设备管理、用户身份、用户与实体行为分析等。

- 零信任安全体系能力

(1) 终端安全

终端安全在零信任体系中，提供访问终端设备的安全状态。终端安全状态，包含多个方面，比如操作系统的版本，补丁更新，软件和进程，安全配置等等。策略引擎平台可以根据这些选项，判断访问终端设备是否达到了策略要求的基线，来决定设备访问的合法性。

终端安全有恶意代码防护软件，桌面管理软件，以及 EDR 等终端安全的软件系统。

(2) 网络安全

网络安全包括，防火墙，入侵检测及防护系统，流量分析系统等网络上常见的安全设备。零信任体系中，安全隔离的理念是在网络层面上完成。

网络安全设备承担策略执行点的角色，接收来自零信任策略引擎的指令，完成网络访问控制动作。用户和设备的持续行为评估，通过分析网络上流量和会话信息获得，并提交给零信任策略引擎。

(3) 数据安全

零信任体系最终的目的就是保护应用和数据的安全。传统静态数据加密，传输数据泄漏防护等安全措施，数据库访问控制与审计，是数据保护的纵深防御机制。

(4) 安全管理平台

零信任体系利用安全管理平台的能力，对整个网络的威胁、日志持续监控和分析，获得风险可视化，自动化响应能力。

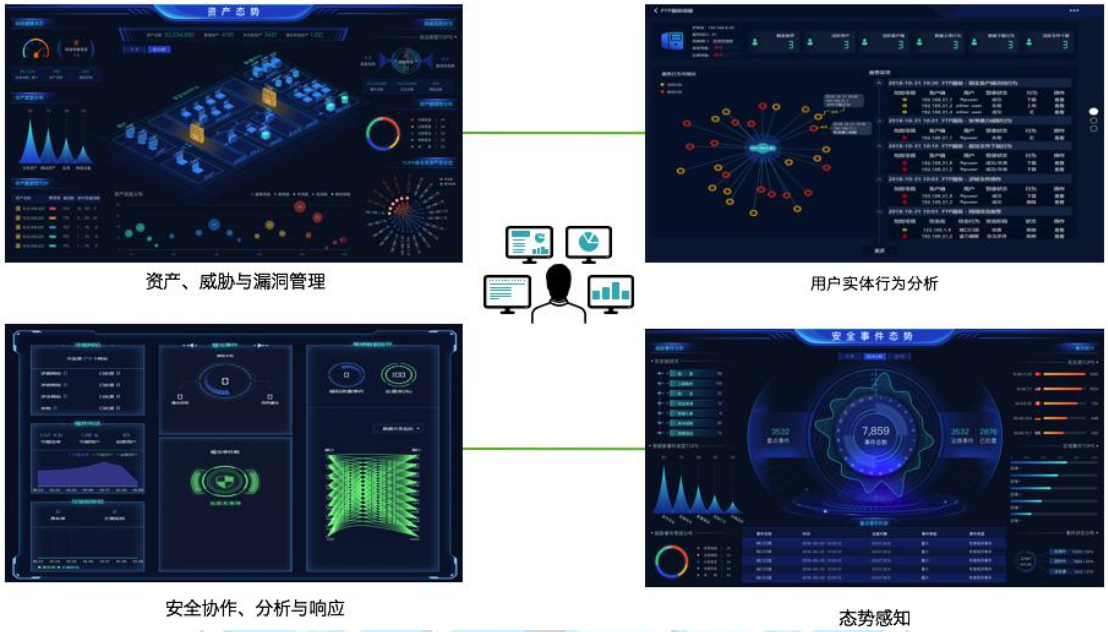

图 27 安全管理平台

安全管理平台包括用户实体分析（UEBA），安全协作与响应（SOAR），威胁和漏洞管理（TVM），以及态势感知平台。

（六）任子行移动应用安全防护平台

任子行移动应用安全防护平台，是基于任子行多年来在互联网监管领域的研发和产业应用，以移动互联网安全管理平台为基础建立的以“1 个平台、4 类检测、4 维监管”为目标，面向政企移动应用安全防护解决方案，全面、系统、深入的解决违法违规移动应用的发现，分析，取证问题，为综合性监管要求提供全面的业务支持。围绕提升移动应用的采集能力，拓展

移动应用的采集渠道，提高移动应用分析的准确性和权威性。为更好解决政企移动应用在研发、发布、运营过程中面对的信息泄露、漏洞挖掘、恶意攻击、仿冒盗版等威胁，提供线下安全技术培训，移动应用加固等服务。

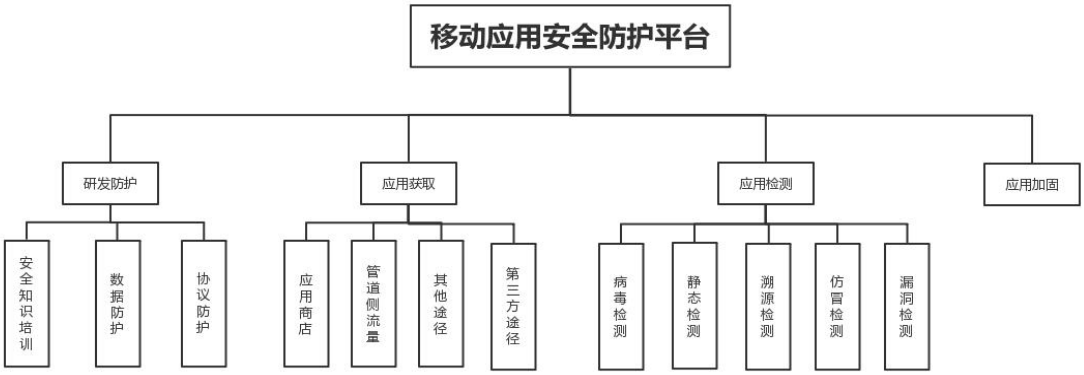

图 28 系统架构图

- 研发防护

安全知识培训：提供基础移动安全基础知识培训，提高开发人员安全意识，并提升开发团队安全水平。

数据防护：提供本地密钥白盒 SDK，为本地 xml、sqlite 等文件中的数据提供加密保护。

协议防护：提供通信协议加密 SDK，对通信数据进行加密、加签保护，防止通讯协议被逆向分析，防止各类刷单、非授权客户端访问行为。

- 应用获取

移动应用商店：包括 PC 端移动应用商店和移动应用商店手机助手;

管道侧流量数据：收集前端捕获的网络流量日志数据；

其它途径：包括 PC 软件下载站，游戏下载网站，论坛，社交软件等；

第三方途径：可以纳入第三方的应用数据。

系统对获取的移动应用展示内容包括应用名称，应用图标，应用简介，应用下载量，应用截图，应用下载链接，应用运营者，应用检测结果等信息。

- 应用检测

系统对获取的移动应用进行检测，识别出恶意应用，按照危险等级，危害类别进行分类。检测手段包括病毒检测，静态检测，溯源检测、仿冒检测、漏洞检测。

病毒检测：使用权威病毒引擎云服务，准确检测代码安全；

静态检测：分为应用权限检测，应用证书检测，应用资源检测，应用代码检测，系统关键权限调用等；

溯源检测：使用模拟器作为运行检测平台，深入分析应用的运行行为，捕获应用服务器 IP、域名等信息；

仿冒检测：对移动应用进行仿冒监测，通过应用名称、包名、签名等信息进行精准识别，及时发现盗版应用在应用商店的分布；

漏洞检测：从业务安全、程序机密性及数据安全方面的用

户登录、密码管理、界面劫持等角度出发对移动应用做全面的扫描检测。

- 应用加固

为政企移动应用提供 Dex 文件加密、So 文件加密，防逆向、防篡改、防调试、防窃取等完整加固保护服务。

（七）深信服 EMM 解决方案

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。

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，具体如图 29 所示:

图 29 深信服 EMM 方案架构

移动应用安全建设问题主要包括：接入安全问题、终端数据安全问题。

接入安全，主要包括以下两大关键问题：

(1) **业务系统防护问题：**业务系统服务器直接暴露互联网，随时可能被扫描、攻击、入侵。

(2) **传输安全问题：**传输过程中明文数据容易被监听、窃取、篡改。

终端数据安全，主要包括以下两大关键问题：

(1) **数据泄密问题：**员工通过截屏、复制、拍照、分享、网络外发、USB 文件拷贝、离职带离企业数据 等方式带来的主动泄密；黑客通过恶意代码、APP 漏洞、病毒、木马、Root/越狱、入侵、恶意 WiFi 劫持、钓鱼 等方式带来的被动泄密。90%泄密事件来源于员工主动/意外泄密。

(2) **风险管控问题:**风险事前如何检测？事中如何阻断？事后如何追溯？

针对安全建设问题，深信服 EMM 方案通过以下多个技术组合来解决，深信服移动安全加固架构如图 30 所示:

图 30 深信服移动安全加固架构

事前事后辅助技术:通过终端环境检测与认证准入方案(事前检测)、应用安全报表方案（事后审计追溯）来做好风险管理；通过业务系统防护方案、传输安全方案来做好接入安全防护。

(1) **环境检测，**通过 ROOT/越狱检测决定终端用户是否可以访问企业数据，一般漏洞都是存在于较低版本的系统，

通过系统版本检测来决定终端用户是否可以访问企业数据。通过对非法 WIFI、非法应用、危险应用检测确认终端环境的安全。

(2) **认证准入，**通过帐号密码/证书、与短信验证码、硬件特征码、动态令牌结合，形成多因素认证方式，防止帐号密码被盗的情况下，依旧能保护帐号的安全。

(3) **接入安全防护，**使用 SSL VPN 接入网关防止业务系统直接暴露在互联网，被扫描、攻击、入侵。使用国产密码/国际商用密码进行对数据传输进行加密，防止被监听、窃取、篡改。使用应用级安全隧道，非授信应用无法访问接入内部网络。

(4) **审计追溯，**通过截屏审计报表、剪切板审计报表、文件外传审计报表、网络审计报表提供更全面的事后审计追溯能力。

事中核心技术方案：设备层强管控、系统层专机专用、应用层双域隔离

(1) 设备层强管控技术方案（CYOD-限制设备外设）

- 外设控制，禁止截屏、禁止拍照、禁止 USB、禁止外置存储、禁止录音、禁止恢复出厂设置、禁止蓝牙、禁止 WIFI、禁止共享热点。

- 应用管理，应用静默安装，应用静默卸载。
- 远程控制，远程定位、远程截屏、远程擦除数据。

(2) 系统层专机专用技术方案（CYOD-限制系统桌面）

- 桌面控制，通过控制开机启动自动进入安全域，来保障专机专用。或者通过调用系统 API 来限制和切换桌面，适用于特定场所只允许使用安全域，离开特定场所允许使用个人域/不限制使用。
- 应用控制，通过配置应用黑白名单，调用操作系统 API，来限制应用的安装和运行，保障设备只能安装/运行工作相关的应用。当希望禁用应用的某个模块/子功能的时，通过调用系统 API 来监控和关闭指定的子模块/子块能。

(3) 应用层双域隔离技术方案（BYOD-限制应用和数据）

- 在终端被 ROOT/越狱情况下，如果应用的内存数据没被加密，可以被 dump 导出，所以我们会对关键内存数据进行加密，通过 I/O 的标准 API HOOK 技术，对落地数据进行透明加密，密钥使用 RSA/SM1/SM4 非对称加密传输，终端使用 AES128 对称加解密，结合文件系统隔离，防止 USB 文件拷贝，恶意程序窃取文件。
- 通过剪切板隔离、分享打开隔离来防止数据外发。
- 通过防截屏、截屏审计、水印技术，来防止截屏外发、拍

照外发等主动泄密行为，以及防止 Android 屏幕监控等被动泄密行为。

（八）天融信移动设备管理系统 TopEMM

移动办公及业务应用安全保障需求日益增长，天融信移动设备管理系统 TopEMM（Enterprise Mobile Management），为客户提供企业移动信息化过程中的整体移动安全解决方案。保障各行业客户在任意时间、任意地点、任意智能终端，能够访问并处理其多种多样的核心业务，打造现代化、高效能企业的安全移动办公系统。员工办公的局限性从时间和空间维度得到了释放，在设备安全、数据安全、通信安全的保障下，企业与员工之间的满意度大幅度提升，工作效率显著提高。平台能够提供移动设备管理、移动应用管理、移动内容管理、移动安全管理，可以与天融信态势感知大数据平台无缝扩容完成移动端业务与办公 PC 端、服务器端等整体安全框架的综合防护。

(1) 天融信移动应用安全接入平台架构

移动应用安全接入平台针对移动终端的终端安全、网络接入安全和移动应用安全、移动大数据安全态势感知四层架构为基础设计，保障移动应用接入安全，具有易实现，安全可靠和分布式操作等一系列优点。

图 31 天融信 EMM 产品技术架构

“四层多维，安全优先”的综合安全运维管理系统以帮助客户建设移动智能统一接入平台为目标，以模块即产品的个性化思维为产品理念，为客户提供全程细粒度的安全防护的天融信移动安全综合解决方案。

安全层：针对移动设备进行安全管理，提高对移动终端的安全可控性，采用安全沙箱技术，为系统建立一个独立的逻辑存储空间，将系统的存储区域与其他应用数据划分开，加固了私密的数据安全性，结合终端病毒查杀、合规准入策略保障终端接入安全。

传输层：在网络传输过程中，针对蜂窝网络，WIFI 环境通过 SSL-VPN 技术，将 APP 与 VPN 的安全 SDK 自动封装，完成沙箱内 APP 启动后自动建立 SSL-VPN 隧道，安全访问内网数据，同时WIFI 控制可保障用户在移动接入时多路径的网络接入访问安全。

管理层：分别针对移动设备安全；移动 APP 安全；移动内容安全；移动通讯行为安全；尤其是移动业务安全提供全面安全防护。

运维层：通过交互层最终将所有安全信息汇总到移动安全风险探知平台，提供终极综合安全手段。

(2) 天融信移动应用安全接入平台功能模块

MDM（移动设备管理）

设备注册后，企业可远程对设备进行管理，包括：设备定位、锁定、擦除；设备的限制、WIFI、VPN、邮箱、加密等安全设置进行统一配置分发；设备合规管理等。

MAM（移动应用管理）

通过企业自有 APP 超市对企业应用进行管理，对企业 APP 做全生命周期管理；对 APP 进行防病毒查杀、漏洞扫描、数据隔 离加密；APP 加固防篡改、安全性评估。通 DEX 加密、开发者签 名校验、配置文件等完整性校验、防止进程附加和安全加壳等，从根本上解决移动平台的安全性问题，高效防逆向、防篡改、防窃取，APP 安全防护水平大幅提高。

MCM（移动内容管理）

企业通过TopEMM客户端对企业移动端文档数据根据用户权限进行显示、推送、下载、删除等全程管理。文档在移动端全

部进行加密处理，隔离存储；文档按照员工注册信息加载水印，完成泄漏追责功能。

MSM（移动安全管理）

结合天融信网络安全技术实力，增加“安全桌面”、“移动门户”、“移动杀毒”、“移动密信（会话加密，限时阅读、阅后即焚）”、“电子围栏”、“VPN 深度整合”等功能，满足客户高级需求的基础上完善移动端安全解决方案，提出天融信自己的企业移动安全管控理念。

（九）卫士通橙讯安全即时通讯协作平台

橙讯是成都卫士通信息产业股份有限公司倾力打造的基于国产商用密码保护的安全可控的即时通讯应用产品及解决方案，提供覆盖“云管端”的一体化信息防护，解决政企行业移动通信和移动办公等业务中的信息安全问题，全面提升用户应对网络安全威胁能力。

橙讯遵循安全为核心的设计原则，从身份认证、数据流向控制、传输加密、存储加密、访问控制、内容追踪、日志审计等多方面出发，采用了基于 SSL/TLS 的双向认证、传输加密技术、PKI 数据加密技术，提供高效、简洁、易用的沟通协作平台，保证应用安全可控。

橙讯已在中央网信办、中国电子科技集团有限公司、成都

市政府等单位成功应用实践，在提升用户的移动办公效率的同时，有效的保障了用户移动业务应用的安全。

橙讯即时通讯平台由橙讯客户端、基础设施、安全平台、服务平台和应用平台组成，其产品结构如图所示：

图 32 橙讯即时通信系统产品结构

基于基础设施、安全平台、密码服务平台及应用平台，构建橙讯应用系统。橙讯客户端可以在专用终端或者自带终端上安装使用，支持主流的移动终端及桌面终端，支持移动端和桌面端同时登录、消息同步收发。

橙讯提供 SaaS 化服务及私有化部署两种模式，其中 SaaS

模式的业务服务器及密管服务器均由卫士通部署及运营，客户无需额外硬件和运维投入，自助开通，注册即用，接入成本低，集成快。各个服务均可采用可伸缩的集群部署模式，满足用户规模增长的需求。系统部署在自主可控的卫士云上，采用云计算技术，所有业务服务器均运行在服务器集群之上，通过虚拟机共享物理主机的计算、存储和带宽资源。各业务服务器均为分布式冗余部署，并配置负载均衡，任意业务单元挂死后，将自动切换到其他实例，系统支持平滑升级和平滑扩容。

橙讯私有化部署的模式为客户单独使用而构建，服务集群部署在客户私有基础设施上，由用户自行管理，保障对数据、安全性和服务质量的最有效控制，资源规模可灵活调配，并可根据客户自身业务做定制开发。

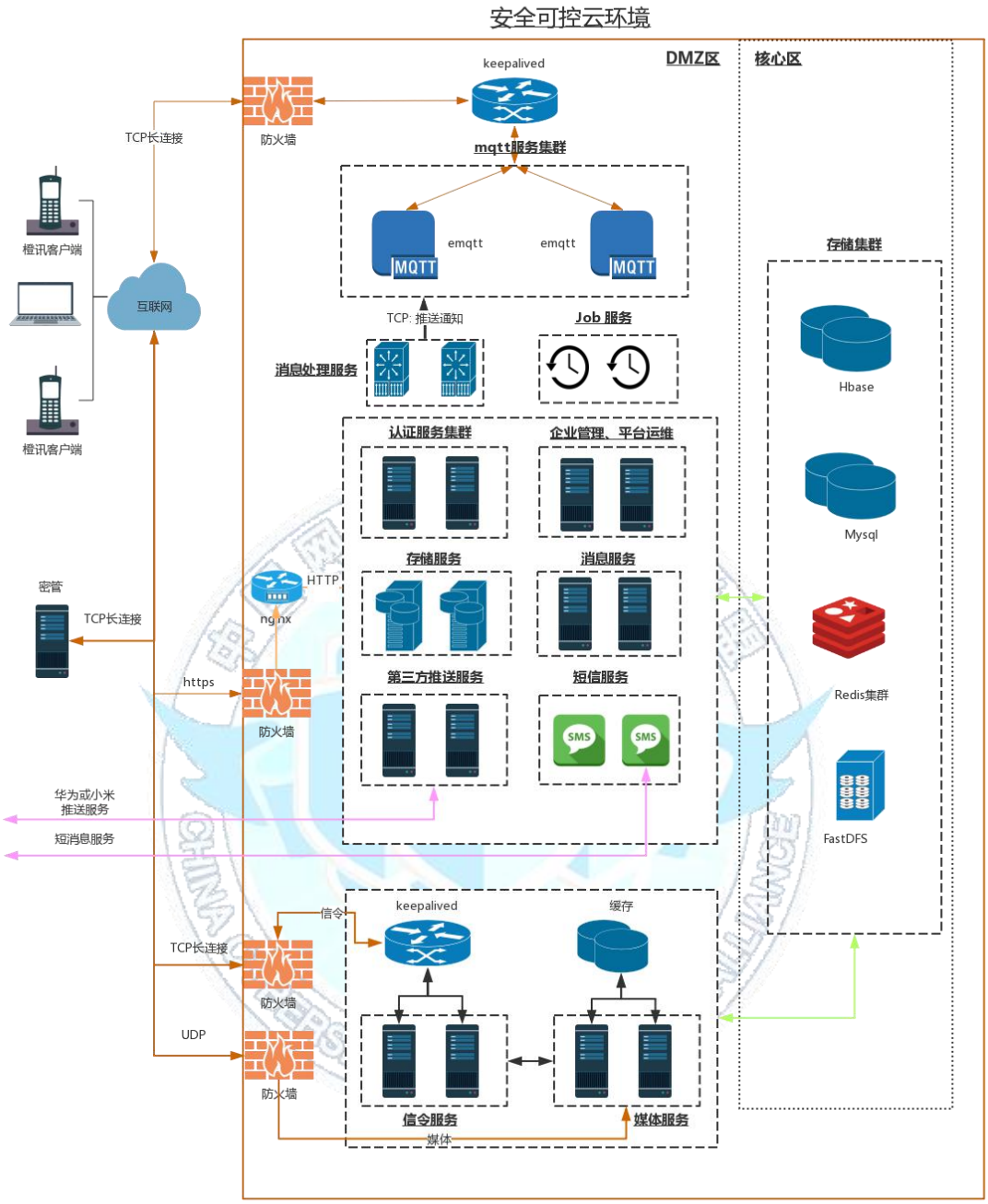

图 33 系统部署组成关系示意图

(1) **加密即时通讯。**支持富媒体消息，包括文本、图片、语音、视频、表情、文件、名片、位置等信息的全程加密收发。

- 公私消息：公有消息转发可溯源，私有消息不支持转发复制。从源头保证消息的全程权限管控。

- 阅后即焚：进入阅后即焚聊天模式，消息读后立即销毁。
- 回执消息：群组会话中能及时了解对方的阅读状态（已读、未读），重要消息，及时反馈。

(2) **加密 VoIP 通话。**实现基于互联网环境下的一对一免费通话。

- 超清音质：采用噪声抑制、回声消除等技术，语音质量远超传统电话。
- 全球覆盖：跨国电话、网络较差时，也能稳定清晰拨打电话。
- 来电名片：接听时，展示同事的来电名片，快速定位联系人，安全无忧。

(3) **组织通讯录。**具备完善的通讯录能力，降低成员间的沟通成本，实现跨部门、跨区域的轻松沟通，助力组织机构快速成长。

- 树状结构：提供树状架构显示方式，清晰展示“组织-部门-子部门-联系人”。
- 快速找人：在真实架构下根据人员属性和层级快速查找人员，无需加好友即可发起聊天，找人快又准。
- 支持超大型组织：百万级通讯录，成员实名制，清晰的组织架构，实现内部人员的安全垂直化管理。

(4) **超大群组。**直击大型组织工作痛点，不再受部门层级人员隔离困扰，快速找到相关人员建群。

- 超大群组：千人超大群组，一键发起群聊。
- 安全聊天：组织内实名制聊天，员工离职自动退群。聊天支持水印，防截图泄露，保障信息安全。

(5) **组织管理。**组织管理员可根据管理及业务需要，自主制定各级管理权限，满足不同层级的政府单位、不同规模的企业组织机构的实际需求。

- 权限粒度化：自定义拥有不同组合权限的管理员，管理权限粒度更细
- 多级授权：从横向和纵向等维度支持组织结构多级授权，保障组织管理有序进行
- 分权管理：管理、审核、安全审计不同的权限根据企业实际管理需要进行有序拆分，保证企业权限制约

(6) **个性化定制。**橙讯不但为组织客户提供了标准的产品能力，面向不同企业还提供了组织个性化设置、开发平台和专属服务团队。

- 应用呈现：根据组织的实际情况，橙讯提供了四种组织定制，分别为：组织 Logo、应用闪屏页、应用引导页、多端图标，使得整个界面更贴合企业组织自身的品牌文化。

- 功能定制：根据组织的特性和需求，在橙讯标准产品功能上，对功能进行新增、修改和删减，让产品更贴合组织的实际工作需求。
- 数据安全：为防止出现操作失误或系统故障导致数据丢失，将全系统或部分数据集合进行异地备份，保证数据的安全和完整。
- 第三方接入：为组织提供强大的应用开发平台，或者提供专属化的第三方应用对接。

（十）北信源安全移动办公平台-信源豆豆 Linkdood

北信源安全移动办公平台-信源豆豆 Linkdood 以“安全连接，智慧聚合”为核心理念，打造跨终端、全方位、安全可信的通信协作聚合平台，以安全即时通信为基本支撑，私有服务器为载体，以开放的、规范化的接口实现移动办公应用的扩展与聚合。通过对通信数据的多重加密防护，保护用户的隐私安全，全面支持 Android、iOS、Windows、MacOS 及国产操作系统，并提供安全协作、协同办公、任务管理、音视频会议、ERP 改造、应用开发、万物互联、互联互通、聚合推广等多层次的平台服务，满足不同行业用户的需求。

北信源安全移动办公平台主要包括 5 个层次：客户端层，网关层，服务层、数据层和监控层。系统架构如下图所示：

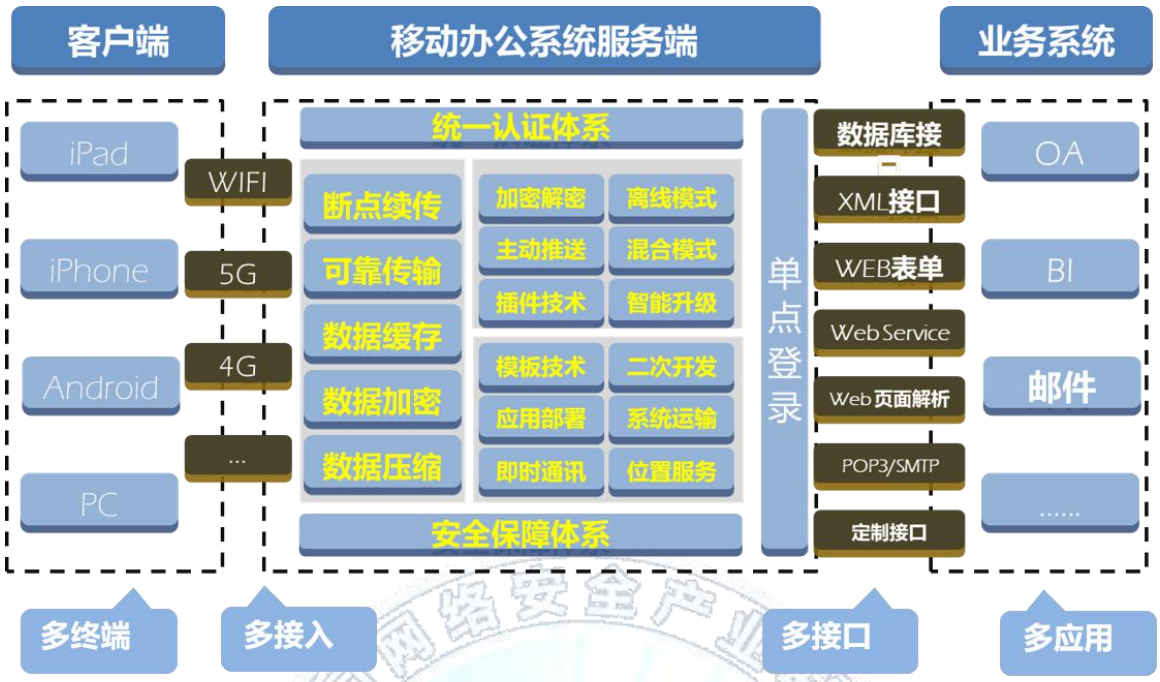

图 34 系统架构图

➢ 安全的即时通信

北信源安全移动办公平台具备完整的即时通信功能，如消息聊天、群聊、语音聊天、语音通话、视频会议、文件传输、微视频等，同时提供签到、审批、云盘、邮箱等扩展应用。除此以外还为用户提供了许多特色的功能，例如:

橡皮擦: 不妥内容，及时擦除。用户可通过发送该指令在获得对方同意的前提下擦除对方聊天记录。在群中管理员可以通过橡皮擦擦除群成员的聊天记录。

阅后回执: 重要消息，及时反馈。自己发送给对方或者群中的聊天内容能够及时掌握阅读状态。

任务调度: 工作任务，及时安排。系统支持在聊天模式下，给对方下达任务调度，及时了解任务执行情况。

延迟消息：定时发送，拒绝打扰。可以将消息发送时间设定为对方方便查看时间段，避免打扰对方休息。

V 标好友：支持用户针对重要的人和群进行标记，即使关闭了系统的全局消息提醒设置，来自 V 标对象的消息也会提醒。

豆豆舆情：为用户提供了舆情大数据服务，用户可以通过设置自己关心的关键词，及时收到豆豆舆情数据。

- 远程移动办公

北信源安全移动办公平台具备考勤打卡、日程管理、工作汇报、工作审批、工作任务管理、群发通知、邮件通知、记事本等完备的远程移动办公功能。

- 数据安全保障

一人一密、三端加密、四维防护！实现从服务器、通信链路至客户端进行数据传送与存储的全程加密，通信数据更加安全!

- 可控的私有服务器

企业用户工作沟通，当然使用自己可控的服务器才安全。北信源安全移动办公平台可灵活部署在私有服务器或云服务器中，支持小到几十，大到上亿用户的不同规模。可以实现真正意义上的您的数据您做主。

- 开放的公共服务平台（DDIO）接口

北信源安全移动办公平台向用户提供了丰富、灵活、多样的第三方办公应用。同时用户也可通过公共服务平台（DDIO）接口改造已有的调度、办公类 IT 应用系统，轻松实现高效便捷的移动办公。

- 完备的 SDK 开发包

北信源安全通信聚合平台为用户提供了完备的SDK开发包，用户可以使用 SDK 与现有的业务、办公等系统进行安全对接，让自己的 APP 快速拥有安全即时通信功能。

- 快速应用开发

北信源安全通信聚合平台使用内置的快速应用开发平台，可为企业快速构建业务应用，满足企业级信息化需求。通过六大核心引擎，可提供 100 多项定制组件功能，以及全可视化的业务应用构建环境。

（十一）奇安信“蓝信”

“蓝信”是移动互联网时代政企专属工作平台，是蓝信移动的核心产品。蓝信平台凭借基于 IM 为统一入口的框架能力和 PaaS 平台的核心技术优势，通过用户体系的三个安全域、百万级通讯录、文档不落地、分级部署、数据总线平台、审计防范、可见性管理、客户端扩展 5、6 屏等产品创新性技术，满足大型、超大型组织的一切工作需要。

蓝信系统架构图如下：

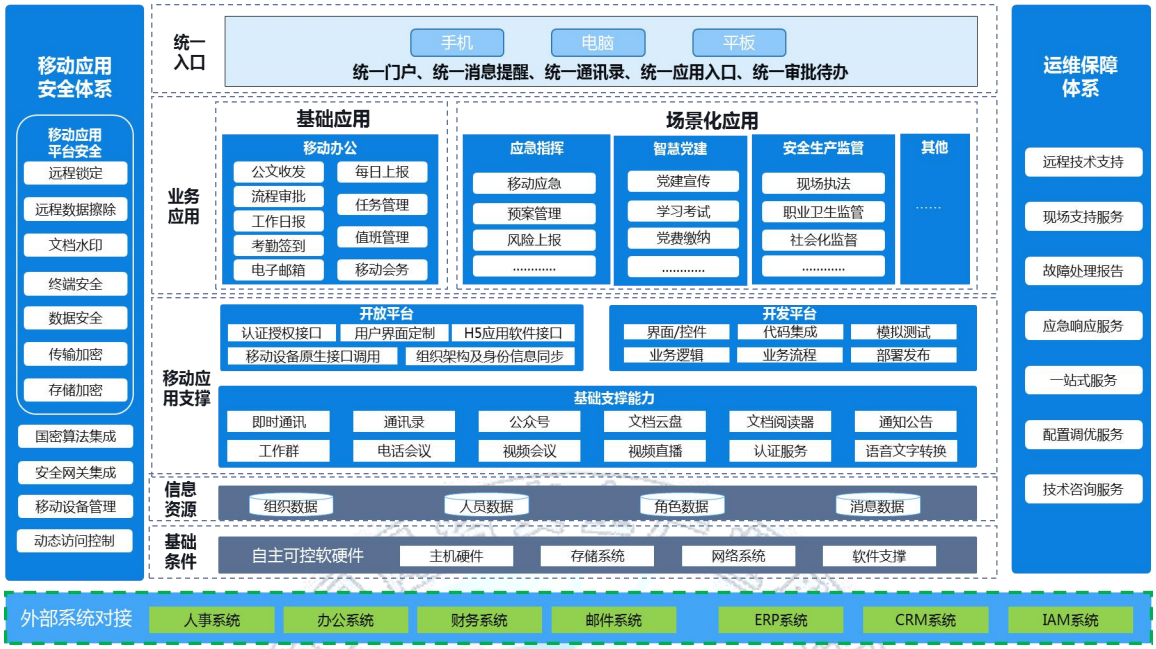

图 35 蓝信系统架构图

蓝信打造“5 横 2 纵”的架构体系。

“5 横”包括：

- 基础条件，包括基础软硬件环境、网络安全软硬件等；
- 信息资源，采集外部系统数据，形成如组织、人员、角色、消息等数据库，为蓝信各业务应用提供数据支撑；
- 移动应用支撑，提供基础服务能力支撑，包括即时通讯、通讯录、工作群，公众号、电话会议、视频会议、视频直播、语音文字转换、文档云盘、文档阅读器、认证服务等；提供广泛的适配接口，提供移动应用的开发平台用于支撑移动应用开发，提供开放平台用于支持对接第三方应用；
- 业务应用，可以对原有系统进行快速集成，如实现公文流

转、审批待办、电子邮件等；也可以根据需求进行快速定制，实现如应急指挥、党建宣传、后勤管理等应用快速开发部署；

- 统一入口，可以使用 PC 客户端、手机客户端、Pad 客户端等通过统一的门户，访问企业应用，访问统一通讯录，接收统一待办消息提醒。

“2 纵”包括：

- 移动应用安全体系，具备国密算法、应用安全、终端安全、数据传输安全、存储加密、远程数据擦除等安全保障手段；
- 运维保障体系，提供远程、现场支持服务，提供故障处理报告，在重大事件中提供应急保障服务等，保障平台稳定运行。

蓝信移动应用安全保障方案具有以下安全特性：私有化部署、应用自身安全、业务安全、认证授权安全、移动数据安全、国密密码安全、移动设备安全、VPN 集成，能够支持私有化部署的系统通过公安部等保 2.0 认证。

(1) 私有化部署

蓝信能够根据用户网络环境进行私有化部署，实现数据本地化，确保敏感数据安全，做到前端保密、传输可控、后台可管。

(2) 应用自身安全

蓝信从系统架构、客户端、服务端存储加密、传输加密、口令存储加密、中间件/操作系统优化、网络安全优化等各个方面提供全面的数据加密与安全保障措施。

(3) 业务安全

在产品业务功能方面，蓝信可提供尽可能丰富的各种应用安全策略，如：可见性设置防止领导联系方式泄露；支持阅后即焚，确保消息安全；远程数据擦除解决手机丢失问题；支持管理员冻结用户，避免风险用户访问系统；支持管理员后台删除离职员工，员工数据实时清除，保护数据信息；全局水印保障消息及文档安全；支持设置屏幕锁；可限制普通用户建立群聊的大小；支持设置组织内敏感词；支持审核公告内容；所有信息转出蓝信，服务器后台记录，满足审计需求；系统对应用进行审核，仅经过审核的应用允许上线等。

(4) 认证授权安全

蓝信可支持提供至少两种用户认证服务方式，如本地用户名口令认证、短信认证、硬件特征码绑定，并可与 CA 及第三方认证系统集成，可通过多种组合，实现多因素认证。

(5) 移动数据安全

蓝信具备追踪设备地理位置、远程擦除数据、文档水印保

护、数据传输加密、数据存储加密、沙盒技术等功能，防止信息泄漏事件发生。

(6) 国密密码安全

蓝信可支持国密算法要求（SM2/SM3/SM4 算法），具备国产密码解决方案,采用具有商密型号的安全密码产品(如软 Key、密码机等），从密钥管理、随机数生成、身份认证、数字签名、数据加密存储等方面进行国产商密算法的应用。

(7) 移动设备安全

在硬件条件具备情况下，蓝信可与 MDM 应用集成，支持对移动设备终端的远程定位，远程数据擦除，远程恢复终端出厂设置等远程控制能力。

(8) VPN 集成

蓝信可支持与 VPN 集成，形成加密网络隧道。蓝信集成的 VPN 支持国密 SM2/SM3/SM4 算法，利用隧道加密技术，对传输数据进行高强度的 VPN 加密，防止泄密和篡改的攻击行为 确保数据安全。

蓝信可支持与 VPN 进行无感知登录的深度集成，实现对移动应用服务的安全使用并保证良好的用户体验。

（十二）筑泰防务移动安全办公解决方案

筑泰防务移动安全办公解决方案基于双模式移动安全终端，

融合移动安全终端管控平台、筑泰加密通话软件、加密文件传输软件、移动指挥调度系统，通过嵌入各行业办公所需的办公软件，有效防止信息泄露，全方位多维度的保护各行业在复杂多变的移动环境中安全高效办公。

移动办公解决方案通过移动安全终端管理平台对业务支撑平台、移动终端管理系统、协同智慧系统、处置管理系统、值守系统进行统一管理。具体方案架构如下图:

图 36 筑泰防务移动安全办公系统架构图

- **移动安全终端**

终端内置加密国产安全芯片，从源头保证信息安全，融合筑泰云端安全操作系统，构建可信的安全执行、传输和储存环境，结合移动安全管控平台，实现自上而下、自内而外的安全隔离加固和保护。

通过国产安全双系统、网络隔离、应用层安全、用户数据安全，全面打造双模式系统的终端。在双模式下，数据以加密形式存储，只能被安全模式中的应用打开或访问，禁止非安全

模式应用访问工作模式的数据和应用。

- **双系统有效隔离**

以系统隔离的形式将一部终端隔离成两个系统，一个生活系统一个安全系统，两个系统之间即共生又绝对隔离，信息、传输和存储均单独存储和运行。

- **移动安全管理**

对移动设备管理、移动应用管理、移动内容管理等功能全面管理，包括应用安全、数据安全、系统安全、网络安全等。

- **指挥调度**

系统软件提供的调度业务分为语音业务和数据业务，数据包括视频、定位、文本、文件等各种数据业务，语音、数据可联合调度。

- **加密通话**

有效防止内部通话遭拦截和蓄意窃听，造成机密信息泄露。通过 VoIP 加密通话软件，实现端到端通话加密，杜绝通话主动或被动泄露。

- **加密文件传输**

自定义数据属性，全网全程跨级控制，定向发送、定时回收、全网销毁、阅读痕迹追溯，通过传播监控，获取人员查阅时间并具有时效性，在规定的时限过后自动销毁。

- **远程移动办公**

通过远程办公 APP 实现网络通话、视频调度、GIS 调度、远程视频会议，现场工作人员将图片、视频实时上传，不受区域限制，提高移动办公应急处理效率。

- **高品质语音通话**

多个终端设备同时通话，音质清晰流畅，不受电磁波的干扰，占用带宽小，不受传输距离限制，只要有网络的地方都可以实现通话。全数字音频处理技术，具有广播、呼叫转移、监听、报警、录音等功能。

- **灵活的视频调度**

支持移动视频图传、视频转发、双向视频电话功能。可将自己的实时视频传达给一个或者多个终端用户，可对视频的流向进行调度，并生成调度记录。

- **丰富的即时通信**

实现类似微信功能和消息推送统一入口，可创建、加入群组，发起交流或群聊，满足每部会商、沟通协同的需要，避免使用公众平台交流工作信息的泄密风险。

（十三）360 金钟罩移动业务威胁感知防御系统

360 金钟罩移动业务威胁感知防御系统，简称（360 金钟罩），是 360 针对于政企单位推出的移动端业务安全管理系统，该系

统采用沙箱的方式为企业移动业务应用进行安全赋能，使其具备移动身份风险检测、移动设备风险检测、移动网络风险检测、移动内容风险检测、移动业务风险操作检测等感知能力，全面保护企业业务数据安全。

360 金钟罩移动业务威胁感知防御系统支持对 Android 业务应用和 iOS 业务应用进行安全赋能。

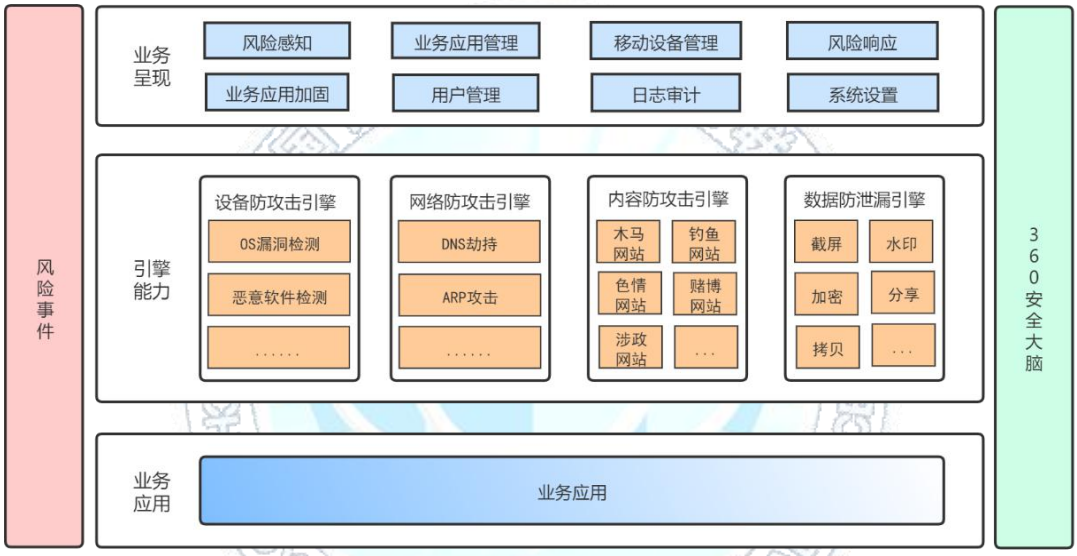

图 37 360 金钟罩移动业务威胁感知防御系统架构图

(1) 业务应用赋能

为保护企业的移动业务应用安全，可通过对企业业务应用沙箱化的方式对移动业务应用进行安全赋能;360 金钟罩移动业务威胁感知防御系统支持 Android、iOS 等业务应用，在业务应用内引入风险感知引擎，如零信任引擎、设备防攻击引擎、网络防攻击引擎、内容防钓鱼引擎、数据防泄漏引擎等，有效感知业务应用运行环境、网络、操作等风险，为企业业务应用保

驾护航。采用业务应用沙箱化的方式为企业移动安全赋能，能够在不干扰原移动业务应用使用的基础上，对移动业务应用进行有效防护。

(2) 业务应用管理

为方便企业对员工所使用的业务应用进行管理，该系统支持对沙箱化后的业务应用进行统一管理，包含对业务应用的分发、阻断访问、恢复访问、数据擦除、删除等，业务应用完整的生命周期管理。

支持多种分发方式，满足用户多使用场景，在无网络或弱网络环境下，可通过安装包下载进行实体安装包分发；在非组织架构人员或访客需访问业务应用时，可通过二维码进行业务应用的快速下载、安装、访问，实现业务应用的高效率、便携性安装；在企业内部，组织架构内的人员，需要进行新的业务应用安装或更新时，企业管理员可通过短信分发的方式，实现多应用、多人员分发，并可根据企业不同部门、人员、群组，做定向分发。

支持对已安装业务应用执行手动阻断访问、恢复访问操作；当业务应用或业务应用所在设备存在风险时，企业管理员可对存在风险的业务应用或业务应用所在设备执行阻断访问操作，当产生风险事件时，保护业务应用数据安全。

支持对已安装业务应用执行手动数据擦除；当安装有业务应用的设备丢失时，企业管理员可以通过此功能远程对业务应用执行数据擦除，及时防止业务应用数据泄露，造成企业相关损失，保护业务应用数据安全。

支持对已上传的业务应用执行删除，可将不再使用的业务应用从管理平台中删除，维护业务应用列表的数据展示。

(3) 业务风险感知

系统支持对业务应用启动期间人、设备、网络、内容、行为等风险进行感知，将风险事件进行大数据可视化联动展示。

- 风险感知趋势图

支持查看近 30 天的风险走势，可查看某一天产生的高、中、低危风险事件数量，并可以按照时间范围进行筛选，查看自定义时间段内的风险趋势及具体的风险事件。

- 基于业务应用维度

可查看业务应用在启动期间所感知的风险事件，并按照不同的风险载体进行分类展示，显示不同风险载体的风险事件占总事件的百分比；按照业务应用感知到的风险事件数量，对业务应用进行 TOP 排行，可快速查看风险事件 TOP 排行靠前的业务应用上产生的风险事件及事件详情。

- 基于设备维度

可查看移动设备上业务应用启动期间所感知的风险事件，并按照不同的风险载体进行分类展示，显示不同风险载体的风险事件占总事件的百分比；按照业务应用感知到的风险事件数量，对设备进行 TOP 排行，可快速查看风险事件 TOP 排行靠前的移动设备上产生的风险事件及事件详情。

- 基于风险类型维度

可查看业务应用启动期间感知到的不同风险类型的风险事件，并按照不同的风险载体进行分类展示，显示不同风险载体的风险事件占总事件的百分比，按照业务应用感知到的风险事件数量，对风险类型进行 TOP 排行，可快速查看风险事件 TOP 排行靠前的风险类型。

- 业务风险响应

360 金钟罩移动业务威胁感知防御系统支持对业务应用所感知的每一项风险，自定义配置其风险响应。当业务应用在启动期间感知到风险事件时，则会根据管理员自定义配置的风险响应，对业务应用进行实时告警、阻断访问等响应，同时也可配置是否通知管理员，可通过短信或邮件通知管理员。

附录 B 术语及名词定义

1. 移动应用 Mobile Application

分为广义和狭义两种定义,狭义的移动应用指用户能够从公开或私有应用市场下载、安装和使用的移动应用程序,广义的移动应用指为支撑移动化应用服务的完整云管端 IT 架构,包括了移动端的狭义移动应用、移动互联网的通信过程、以及提供移动应用服务的软硬件资产。广义的移动应用包含了狭义的移动应用。

2. 行业移动应用 Industrial Mobile Application

特指各重点行业的 B2E 面向雇员的移动办公和移动应用场景,区别于 B2C 的个人消费移动应用,行业移动移动办公和移动业务场景往往建立私有化的应用市场,进行移动应用 APP 客户端的安全加固、发布、推送、更新等应用生命周期管理。

3. 企业配发设备 Corporate Owned, Personal Enabled

由企业统一选型、采购、配发的移动终端设备,设备归属权属于企业,用于完成业务和办公操作,不涉及员工个人隐私保护,可以执行设备级管控策略。

4. 个人自携设备 Bring Your Own Device

员工个人移动终端设备,设备归属权属于员工个人,可安装和运行与工作有关的移动应用客户端软件,在 BYOD 设备上执行设备级管

控策略，会影响到设备上个人隐私保护，通常采用面向应用的应用级管控策略，只作用于与工作有关的应用和数据保护。

5. 安全工作空间 Secure Workspace

在 BYOD 设备上的一种移动办公门户形态，安全工作空间中只包括受保护的移动办公应用和数据，构成了 BYOD 设备上的工作域，应用级安全管控策略只作用于工作域,避免与个人域中的个人应用和数据的隐私保护发生冲突。

6. 企业移动管理 Enterprise Mobility Management

国际咨询机构 Gartner 面向移动业务安全保障提出的能力集合，包括了移动设备管理 MDM、移动应用管理 MAM、移动内容管理 MCM、移动身份管理 MI、以及容器化技术等内容，是移动安全领域内相对权威的一种方法论参考。

7. 国密算法 National Cipher Algorithm

即国家密码管理局认定的国产商用密码算法,其中包括了对称加密算法 SM1/SM4，椭圆曲线非对称加密算法 SM2，杂凑算法 SM3 等，在政府等敏感行业内可能会有使用国密算法的特殊规定。

8. 单点登录 Single SignOn

简称为 SSO，是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。实现 SSO 需要在各应用系统与身份信任服务基础设施之间进行集成。

参考文献

[1] 中国互联网络信息中心 第 43 次《中国互联网络发展状况统计报告》

[2] 中国互联网络信息中心 第 44 次《中国互联网络发展状况统计报告》

[3] GA/T 1466.2-2018《智能手机型移动警务终端 第 2 部分：安全监控组件技术规范》

[4] 《司法行政移动执法系统技术规范》（送审稿）

[5] 《中华人民共和国网络安全法》

[6] GB/T 35273-2020《个人信息安全规范》

[7] GB/T 22239-2019《网络安全等级保护基本要求》

[8] GB/T 23927-2016《信息安全技术 移动智能终端安全架构》

[9] 第一财经商业数据中心&钉钉《2019 中国智能移动办公行业发展趋势报告》

[10]第一财经商业数据中心《2018 中国移动办公安全微调查报告》

[11]YD/T 2439-2012《移动互联网恶意程序描述格式》

[12]通付盾移动安全实验室《2018 年度移动应用安全态势报告》

[13]腾讯安全科恩实验室《2018 年 Android 应用安全白皮书》

[14]中国网络安全产业联盟《移动互联网应用程序安全规范》

[15]赛迪智库&通信产业报《5G 十大细分应用场景研究报告》

[16]华为《5G 时代十大应用场景白皮书》

[17]信通院《5G 应用创新发展白皮书》

[18]中国移动《5G 安全白皮书》

[19]中国移动《重大突发公共卫生事件网信安全法律风险合规指引》