可信移动企业安全环境

企业移动终端安全管理解决方案探讨

内容安排

1. 移动终端安全管理需求
2. BYOD解决方案简介
3. “可信移动企业安全环境”方案简介
4. 众筹方案介绍

移动智能终端使用日益广泛

- 出货量越来越大
  - 台式电脑基本停止增长
  - 笔记本电脑、平板电脑经过初期的快速增长之后进入缓慢增长阶段
  - 智能手机飞速增长
- 访问更多企业业务系统
  - 电子邮件
  - OA、CRM、ERP等经营管理系统

移动终端安全性越来越受重视

- 数据泄露的风险更高
  - 和笔记本电脑等相比较，更易丢失
  - 安全保护措施普遍较差，很多人的手机根本不设密码
  - 由于智能手机价值更高，黑色产业链将目标向Android类终端转移
    - 大量手机病毒传播者使用远程控制的手法，在中毒手机上安装推广软件、后台订购付费服务、窃取用户手机里的个人信息

数据防泄露成为热点问题

- 棱镜门事件，发生在信息技术最发达，信息安全最为重视的美国政府
- 近年来，其它移动终端相关数据泄露或安全事件

序	泄密事件	点评
1	苹果手机上传用户隐私数据	涉及6亿部iOS设备，可上传照片、浏览记录和GPS定位等数据
2	安卓4.4以下版本存在的应用签名冒用漏洞	涉及十亿以上的4.4版本以下的安卓设备
3	安卓4.4以下版本存在的敏感信息泄露漏洞	黑客可能借此获取用户的敏感信息，包括银行服务和虚拟专用网络(VPN)的密钥，以及用于解锁设备的PIN码或图形
4	2013年7月，Bluebox Security发现安卓系统重大漏洞，恶意开发人员可以修改任何APK代码，同时不破坏其签名	黑客可能将任何一款合法软件变成“僵尸程序”，获取设备的控制权和数据
5	搜狗手机输入法漏洞导致大量用户信息泄露	移动应用漏洞利用导致泄密情况值得警惕，微信漏洞泄密个人关系图谱也证明该问题。
6	WhatsApp聊天记录安全漏洞	其它获得SD卡读取权限的应用可读取明文的WhatsApp聊天记录，导致用户隐私泄露

现有主要解决方案（MDM）（1）

- 操作系统支持
  - iOS、Android、Win8
  - 以iOS和Android为主，被有意无意忽略的Wintel
- 主要功能
  - 资产管理：信息采集、远程管理（设备定位）
  - 接入管理：统一网络配置（802.1x接入、VPN接入）
  - 软件管理：企业应用商店、黑白名单
- 安全管理
  - 邮件安全
    - 具有加密存储的邮件客户端，支持常见协议如Exchange/POP3/IMAP等
  - 内容安全：加密存储、沙箱、虚拟机
  - 远程数据安全：数据擦除、设备锁定

现有主要解决方案（MDM）（2）

- 面临的困难
  - Android
    - 版本“碎片化”，难以统一支持多版本
      - 在中国，华为、中兴、宇龙酷派、小米等市场占有率高，使得版本更多
    - 高质量的应用比较少，对开发者和厂商吸引力不足
    - 运行在Java虚拟机中，无法对硬件、操作系统底层做进一步控制
  - iOS
    - 封闭系统，开发应用难度较高
    - 受限制非常多
      - 无法后台运行
      - 无法介入现有App的运行
  - ROOT权限问题，安全类软件，往往需要取得Root权限
    - ROOT权限的取得困难，使得系统的部署困难

MDM类方案，根本的问题在于

- 在属于个人的设备（BYOD）上，要去做过多的控制
  - 静默安装、删除软件，个人防火墙控制，服务控制等，往往需要Root权限或越狱
  - 容易产生隐私冲突：如通信录、个人照片、聊天记录审计等
- 移动终端，最初的设计是以个人用户为目标
  - 以减少操作复杂性为目标，缺乏企业级特性
  - 近年来随着移动终端在企业的应用，苹果、三星等才逐步引入一些企业级特性
- 过多的OS版本（Android、iOS、Windows），开发和兼容性测试根本无从谈起
  - Android之上，各个厂商又有自己的版本
  - 每个发行版本，又有子版本
- 国外MDM厂商的方案主要关注防止被动泄密
  - 如防丢失之后的泄密，防入侵之后的泄密等
  - 但基本无法解决中国企业最担心的（合法）使用者主动泄密的问题

怎么办？

- 让上帝的归上帝，凯撒的归凯撒
- BYOD设备
  - 产权属于个人，决定了企业不适合在其上做过多的管理和控制
  - 给BYOD设备一个准确的定位，员工自有设备，顺带用于处理单位的业务
    - 给BYOD以合适的网络访问权限；
    - 给BYOD以适度的管理控制；
    - 以不侵犯员工隐私、不损害员工利益（违反保修规定）为前提；
    - 主要关注防止被动泄密
- 核心业务系统，需要移动终端，怎么办？
  - 单位负责采购终端，配发给员工
    - 定制硬件系统、定制安卓OS系统、定制移动应用等
    - 选择双系统的终端、定制安卓OS系统、定制移动应用等
  - 既防止被动泄密，又防止主动泄密

定制系统操作系统选择

- iOS
  - 封闭系统，无法定制
- 安卓
  - 开源系统，可定制
  - 存在一些已知风险和漏洞，需要解决

安卓系统安全性分析

- 系统安全
  - Linux内核安全——主要关注驱动程序尤其是硬件驱动程序的安全
  - 系统库安全——原生系统库可能存在漏洞
  - Dalvik虚拟机——可能通过不安全的字节码攻击虚拟机
- 应用安全
  - 应用程序权限——终端用户无法判断哪些权限是必要的，带来隐患
  - 利用安卓共享用户ID机制和相同签名证书获取权限
  - 应用程序安装——多种途径，有一些途径可能带来风险
  - 网络浏览器——恶意脚本攻击浏览器，获取浏览器的权限
  - 数据库与SQL 注入——读取安卓系统数据库中敏感的数据
  - 软件更新——更新系统到一个有已知漏洞的版本

安卓系统风险与漏洞

- 已知安全风险
  - 非法获取root权限
  - 非法获取安卓系统权限
  - 应用签名机制漏洞
  - 密码安全问题
  - 浏览器下载恶意软件
  - 无线传送恶意软件
  - 破坏性网站或链接
  - 锁定SIM卡
  - 丢失硬件组件或导致硬件功能紊乱
- 潜在安全漏洞
  - 安卓源代码公开被发现的漏洞
  - 安卓原生系统库和Linux内核漏洞
  - 应用框架漏洞
  - 应用程序授权漏洞
  - 文件系统漏洞
  - 通过网络传播的漏洞
  - 通过外设传输的漏洞

定制安卓系统企业级安全特性

- 可信硬件
  - 与有实力的硬件厂商合作定制
  - 不允许终端用户刷ROM
- 可信操作系统
  - 深度定制开源安卓操作系统，去掉不必要的组件和系统库
  - 不允许终端用户获得root权限
- 可信应用软件
  - 只能通过系统定制的应用商店安装应用软件
  - 只能运行通过系统定制的应用商店安装的应用软件
- 可信通信信道
  - 自动识别网络状况，选择最合适的接入方式安全的接入企业内网
  - 既验证终端用户、设备信息，也验证接入的网络是否安全

具体解决方案

- 定制硬件（不允许终端用户root和刷ROM）
- 定制安卓操作系统（ 不允许终端用户升级系统版本）
- 回收root权限（系统自身进程不受限）
- 仅能通过系统内置的应用商店安装应用程序，不允许通过其它任何方式安装第三方应用程序
- 只允许通过加密的或安全的网络信道访问相关业务系统
- 对外设进行管控
- 加密文件系统
- 强制安全策略，如：
  - 强制自动锁屏
  - 强制密码策略

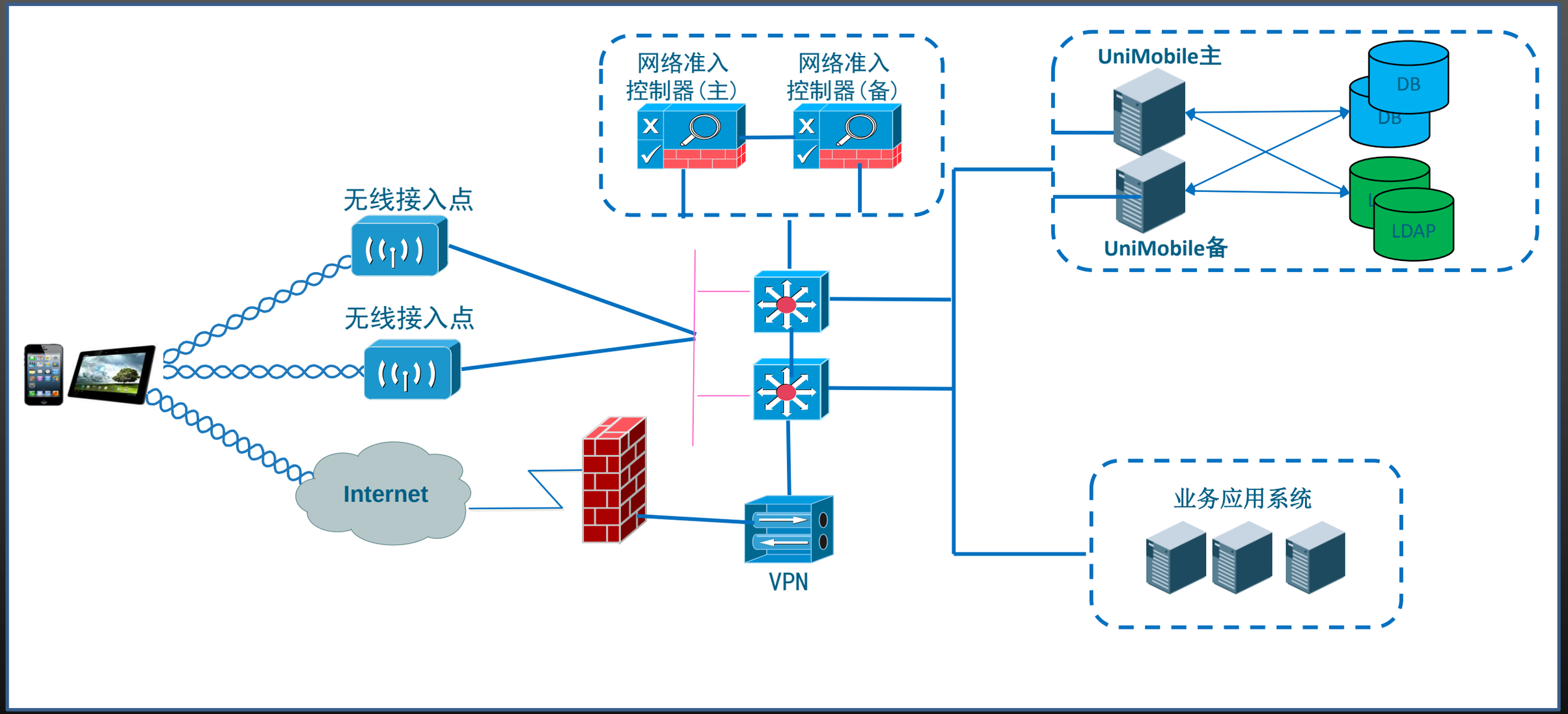
内容安排

1. 移动终端安全管理需求
2. BYOD解决方案简介
3. “可信移动企业终端安全环境”方案简介
4. 众筹方案介绍

BYOD设备管理总体方案

- 准入控制
  - 802.1X、Portal方式
  - 按帐号给移动终端授权“所能访问的网络资源”
  - 与联软UniNAC方案完全融合
- 提供无需Root权限的管理功能
  - 注册服务管理
  - 企业应用商店
  - 远程管理
    - 远程定位、远程锁屏、远程消息推送
    - 远程查看设备信息
- 提供统一的移动终端APP安全开发框架
- 支持iOS/Android/Windows

部署示意图


网络准入
控制器(主)
网络准入
控制器(备)
UniMobile主
DB
DB
UniMobile备
LDAP
无线接入点
无线接入点
Internet
VPN
业务应用系统

部署方案简介

- 支持各种移动终端的管理
- 单通信服务器支持10万以上终端管理能力

内容安排

1. 移动终端安全管理需求
2. BYOD解决方案简介
3. “可信移动企业终端安全环境”方案简介
4. 众筹方案介绍

总体思路

建设思路

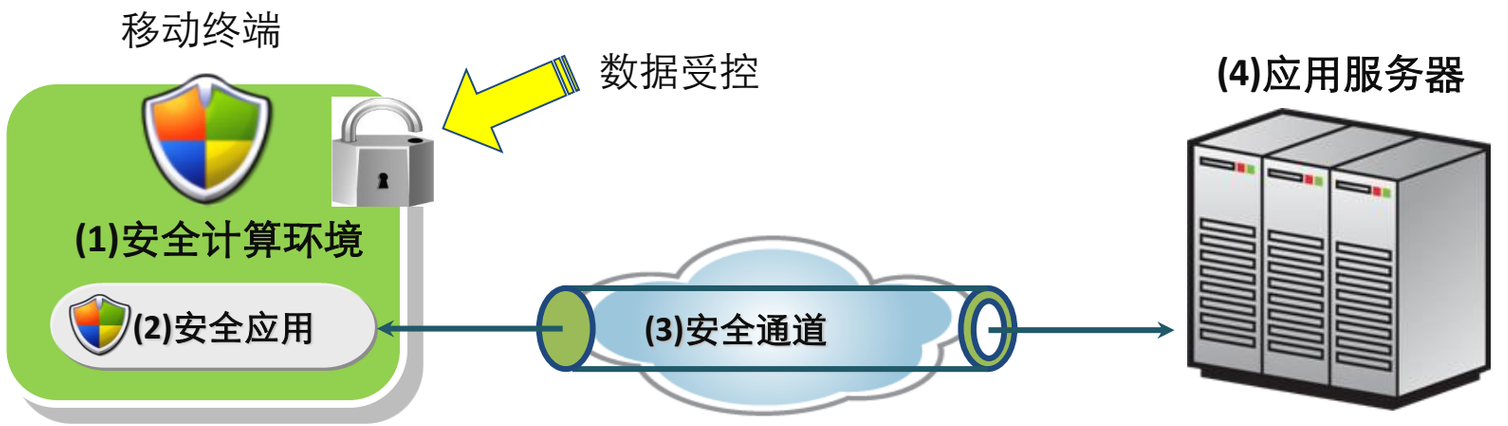
总体规划，顶层设计，分而治之，分步实施

- 最终建立一套集中统一的安全管控平台，涵盖：台式PC、笔记本电脑、平板电脑、员工智能手机在内的所有终端设备

建立端到端的企业安全环境

- 对于不同来源的终端设备，采取不同的技术方案
- 移动终端、传输通道、企业应用之间，建立一个闭环体系
- 实现端到端的企业安全环境，确保企业的数据安全

端到端安全



系统架构

可信移动终端计算环境

定制App（适用于BYOD）

- 企业应用
- 其它应用
- 应用商店
- 移动安全SDK
- 远程管理

定制OS系统（企业配发）

- 应用商店
- 安全合规管理
- 远程锁定
- 远程擦除
- 远程外设
- 远程防火墙
- 加密存储文件系统

虚拟化移动终端

- 虚拟化远程控制客户端
- 防止截屏拷贝
- 远程控制协议 SRMP Over SSL

接入控制

- 网络智能配置与准入
- 身份验证
- VPN接入
- 无线802.1x接入

移动终端管理系统

- 远程管理
- 应用发布管理
- 网络准入认证与合规性
- 资产管理模块
- 安全策略与合规性管理
- 报表统计模块
- 基础功能模块（客户端更新/权限/组织架构/监控等）

- 安全网关
- 云存储（数据集中存储）
- 虚拟化平台（移动操作系统）

技术方案

- 移动终端侧
  - 基于Android操作系统4.4，进行定制
  - 开发系统基于Google Nexus 7（实验系统，支持与其它厂商合作定制）
- 管理后台
  - 管理系统：基于成熟产品管理后台，为移动终端管理优化
  - 服务器：Linux服务器
- 主要创新点
  - 大并发通信基础组件
  - 在Android系统上，实现类似黑莓的安全性

定制终端安全特性(1)

- 定制的移动终端，只能
  - 接入特定的、经授权的网络
  - 运行指定的软件
  - 访问指定的应用服务器
  - 在本地编辑、处理文档
    - 文档在本地加密保存
    - 只能在本地存储器和指定应用服务器间流转
- 以下操作，员工个人非授权不能进行
  - 安装、卸载软件
  - 访问非授权IP
  - 访问USB、蓝牙设备端口

定制终端安全特性–接入控制

- 智能识别网络场景
  - 自动发现可信的网络SSID，自动接入
  - 自动启动Portal认证
  - 自动启动VPN客户端
- 双向验证设备与网络的证书
- 支持多要素关联绑定
  - 用户帐户、设备、网络

定制终端安全特性-OS定制

- 开机启动画面
- 文件系统加密
- 精简系统组件
- 关闭非必须外设端口
- 关闭非必须服务进程
- 桌面背景定制
- 企业集中控制的移动终端防火墙

支持的移动终端硬件平台

- 原型系统基于Google Nexus 7开发
- 3G/4G通信模块，可选

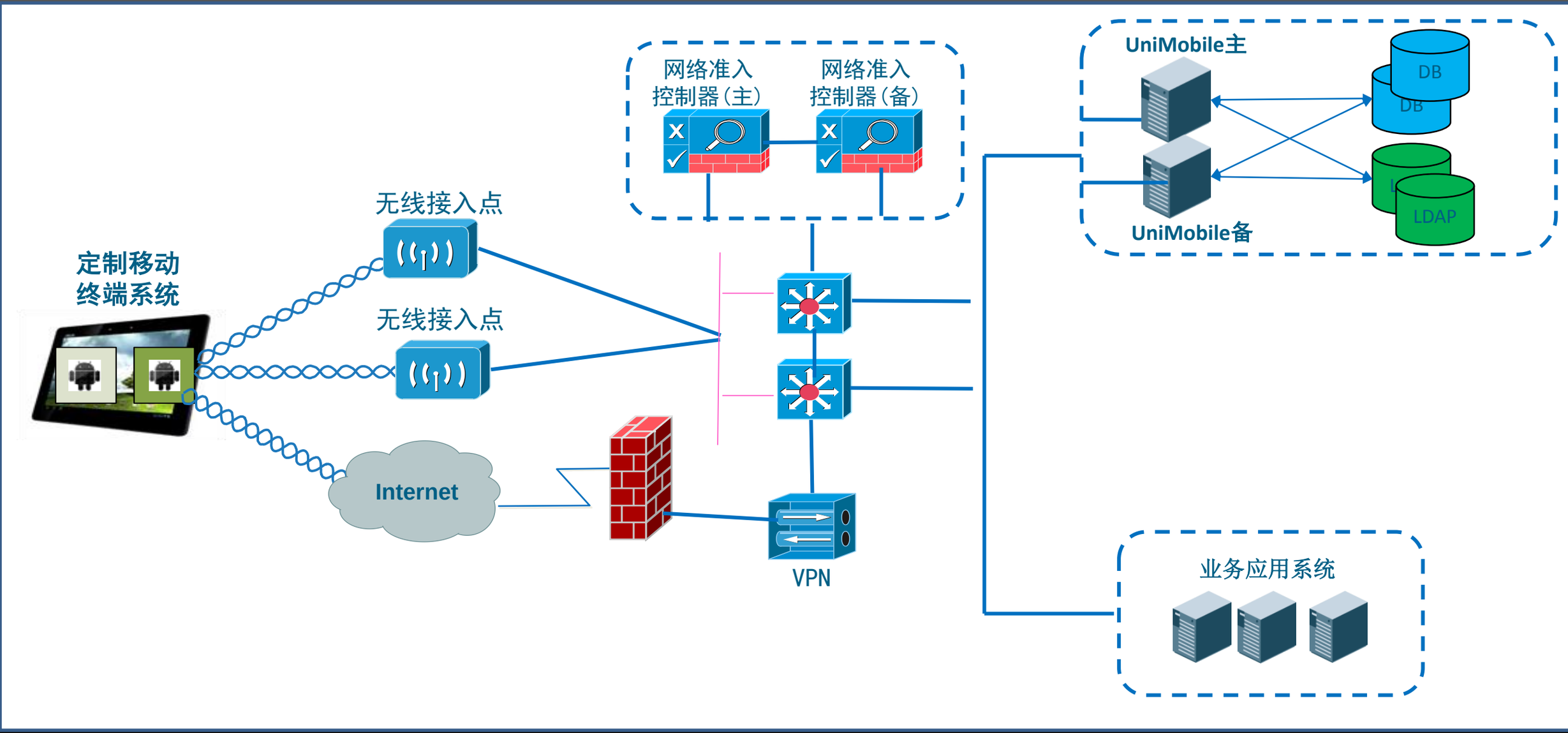
应用集成

- 企业应用商店（App Store）
- 移动终端基础管理功能
  - 远程管理
  - 设备信息
  - 外设及端口管理
- VPN Client
- 其它企业定制应用

管理后台

- 基于Linux平台
  - OS、DB、应用中间件等，均基于开源系统定制
- 支持双机热备
- 系统容量
  - 单通信服务器支持10万以上并发
  - 支持分级部署和云部署模式
- 后台管理系统
  - 策略设置
  - 系统报表
  - 审计信息

部署示意图


网络准入
控制器(主)
网络准入
控制器(备)
UniMobile主
DB
DB
LDAP
UniMobile备
无线接入点
无线接入点
定制移动
终端系统
Internet
VPN
业务应用系统

演示

- 1、VPN连接演示
- 2、应用下载
  - 安装一个APP，不提供其它应用商店
- 3、防火墙功能演示
- 4、本地文件加密演示
- 5、远程管理
  - 远程定位
  - 远程锁屏
  - 远程消息推送
  - 远程查看设备信息

内容安排

1. 移动终端安全管理需求
2. BYOD解决方案简介
3. “可信移动企业终端安全环境”方案简介
4. 众筹方案介绍

众筹方案介绍

- 需求
- 解决方案
- 定制产品
- 运营

谢谢！