无安全　不移动

-BYOD的趋势与挑战

谈 晶

HUAWEI

BYOD趋势

BYOD下的安全挑战和对策

华为移动办公实践分享

一个移动的社会

487M 2011年智能手机发货量，首次超过PC发货量

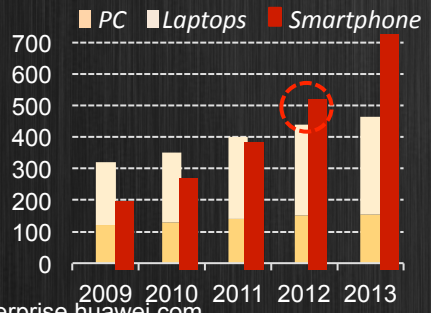
1.2B 2013年移动员工的数量

50% 以上连接到公司网络的移动设备为员工自带Smartphone和平板电脑

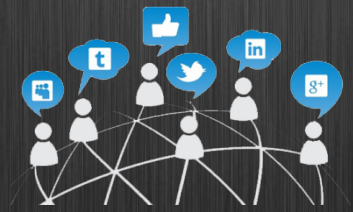
17% BYOD用户数占办公人数的比例

移动的驱动力

移动设备

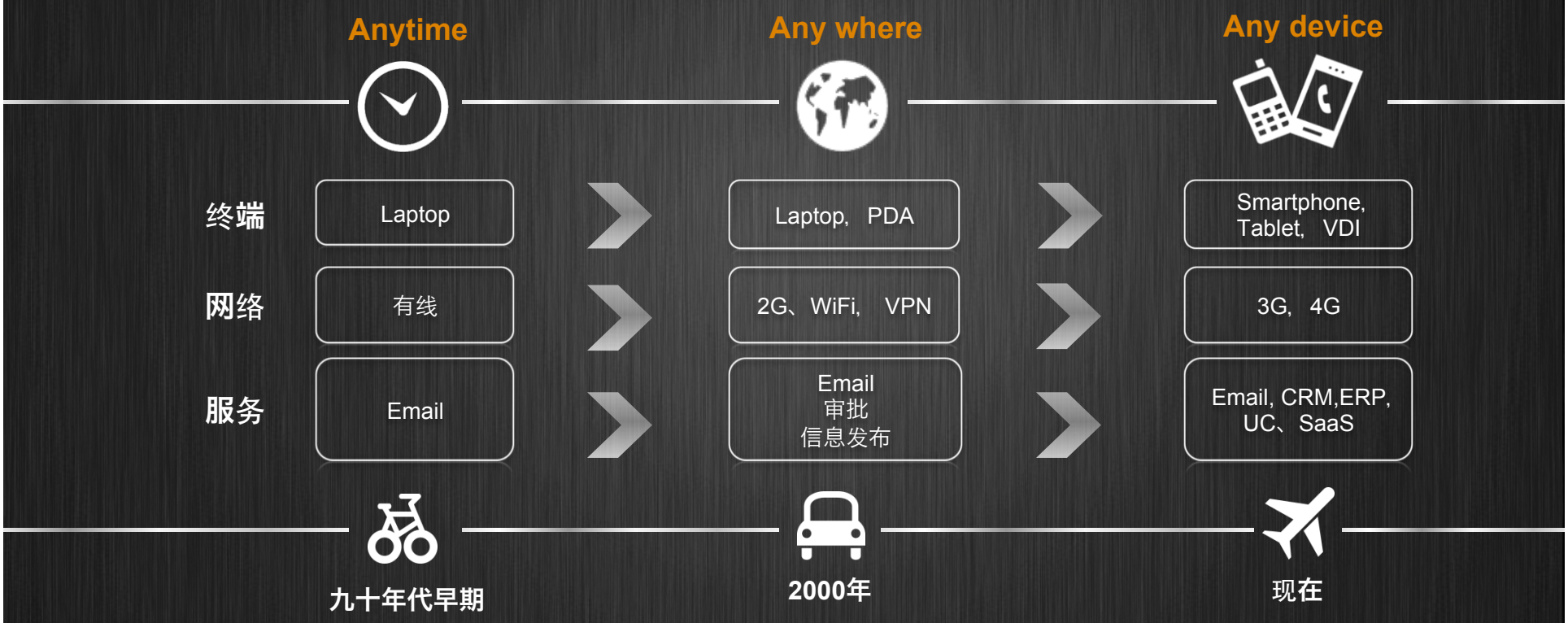


APP应用



人员

移动办公不断带来更大的自由

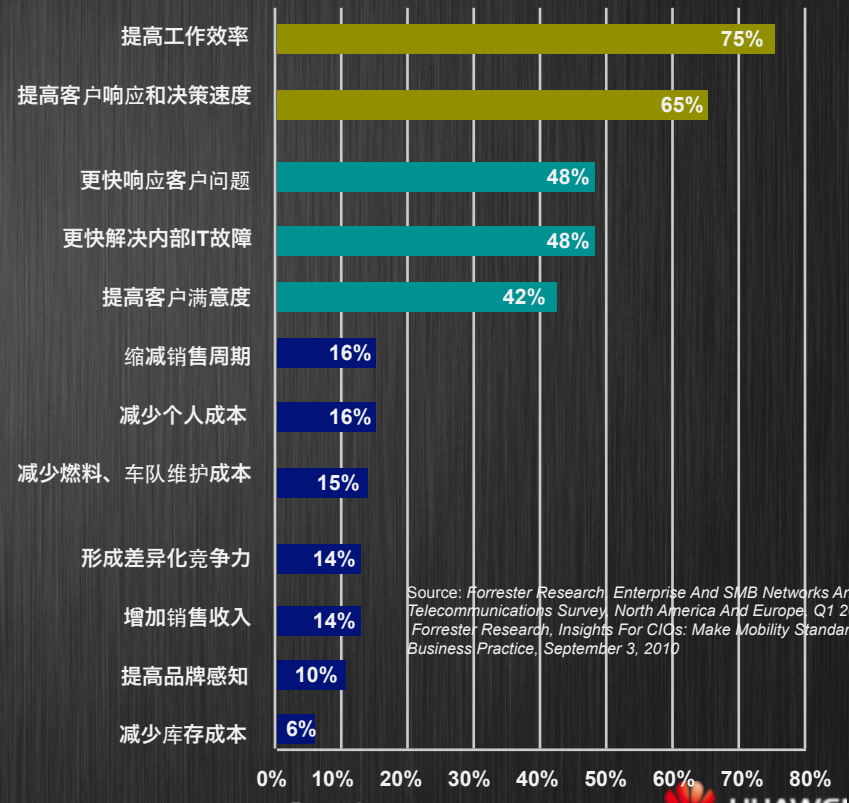


BYOD给企业带来的价值

- 提高员工的工作效率
- 快速决策
- 更快响应客户问题
- 提高客户满意度
- 降低成本

....

What Benefits, If Any, Has Your Firm Experienced as a Result of Deploying Mobile Applications?



Source: *Forrester Research, Enterprise And SMB Networks And Telecommunications Survey, North America And Europe, Q1 2010 Forrester Research, Insights For CIOs: Make Mobility Standard Business Practice, September 3, 2010*

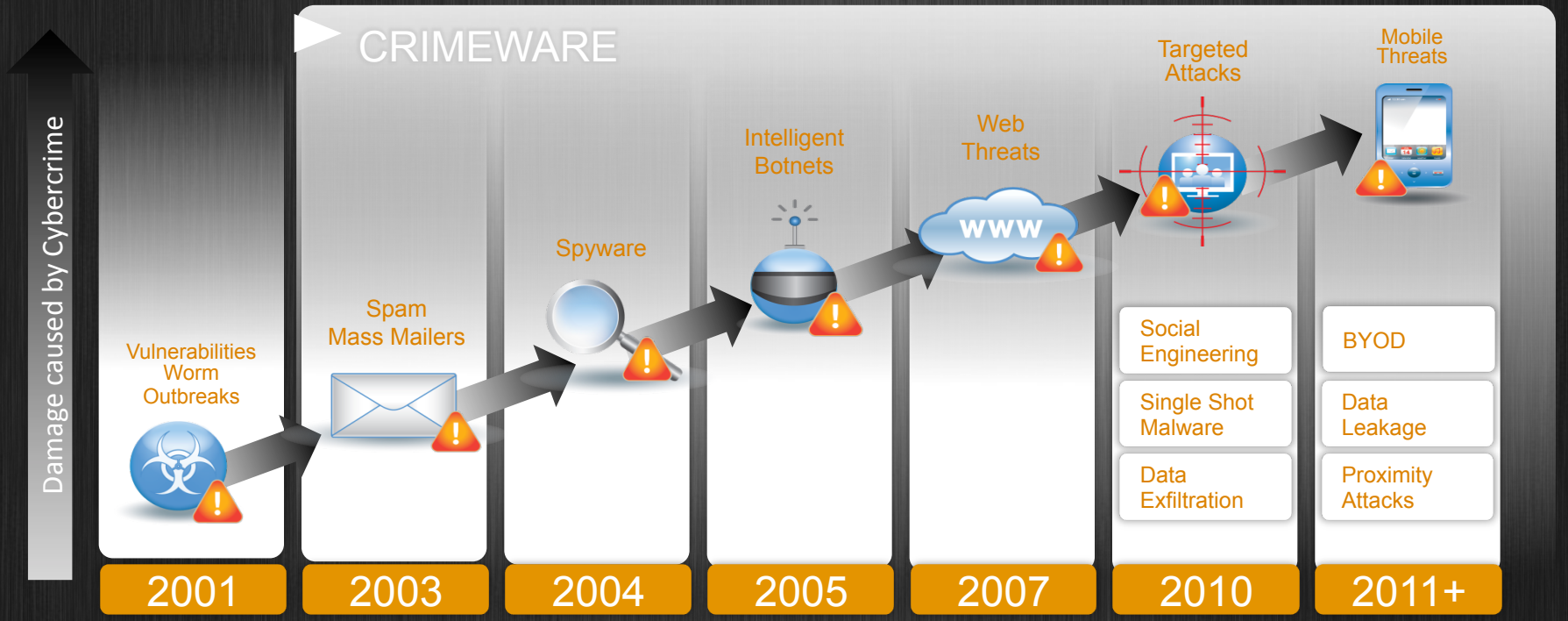
BYOD趋势

BYOD下的安全挑战和对策

华为移动办公实践分享

威胁的演进2012

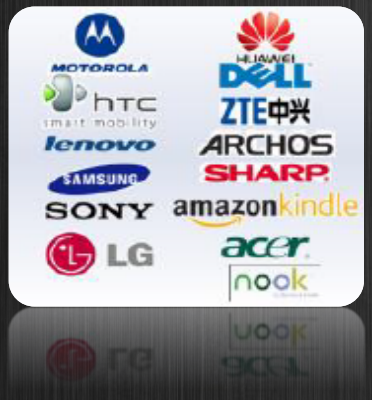
Evolution to Cybercrime



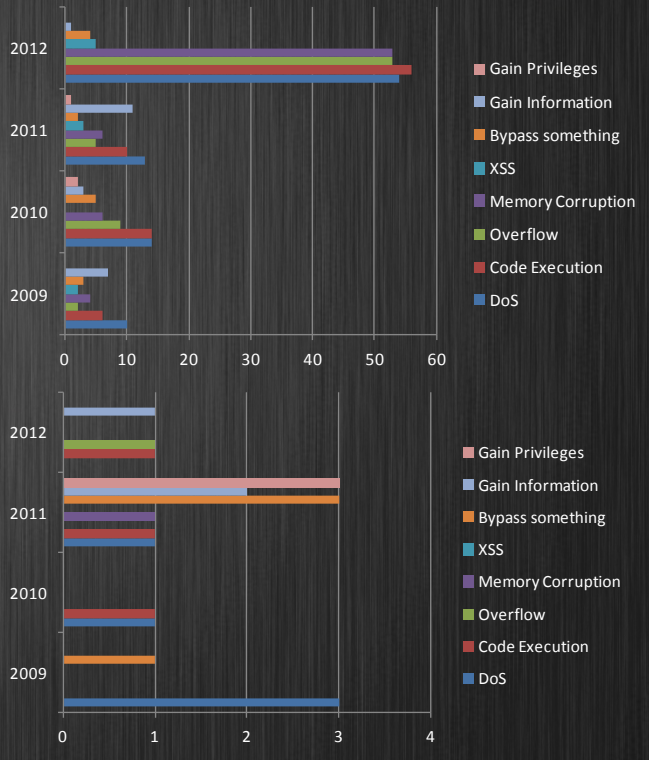
Source: 2012 Trend Micro Inc.

异构移动环境引入新的安全漏洞

15+移动设备厂商，5+移动平台，100+平台漏洞



Top1风险：丢失设备在弱安全保护下的数据泄漏

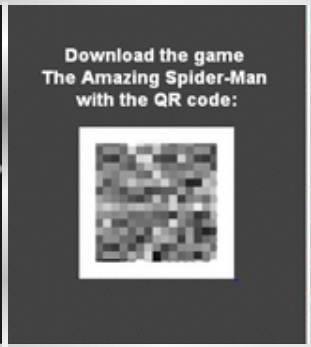


移动信息泄密风险增加

47%的企业有敏感资产存储在智能终端上

- 员工安全意识欠缺
- 设备被盗丢失，存储数据外泄
- 不安全的网页浏览
- 不安全的WiFi、蓝牙连接
- 补丁升级不及时导致被入侵

个人应用下载引入安全风险



伪造的蜘蛛人APP下载页面

- 2012是移动应用年
  122万＋移动应用
  数10亿＋次的下载
  参差不齐的应用质量和安全性

- 应用的漏洞
- 应用分发的风险（Android Market）

随意下载移动应用带来数据泄密风险，增加企业管理和支持负担

BYOD和企业IT策略间的落差

传统安全策略

- 两个主流的OS：Windows, Apple
- IT管理员统一的设备部署路径
- IT管理员统一部署桌面应用
- 成熟的安全管理策略和技术：AV/IPS、补丁、LCM等

BYOD的特点

- 5＋移动OS
- 移动设备的部署路径：运营商
- 移动应用的部署机制：OTA、工厂预装
- 安全策略：传统策略难以移植、策略强制缺乏成熟技术支撑

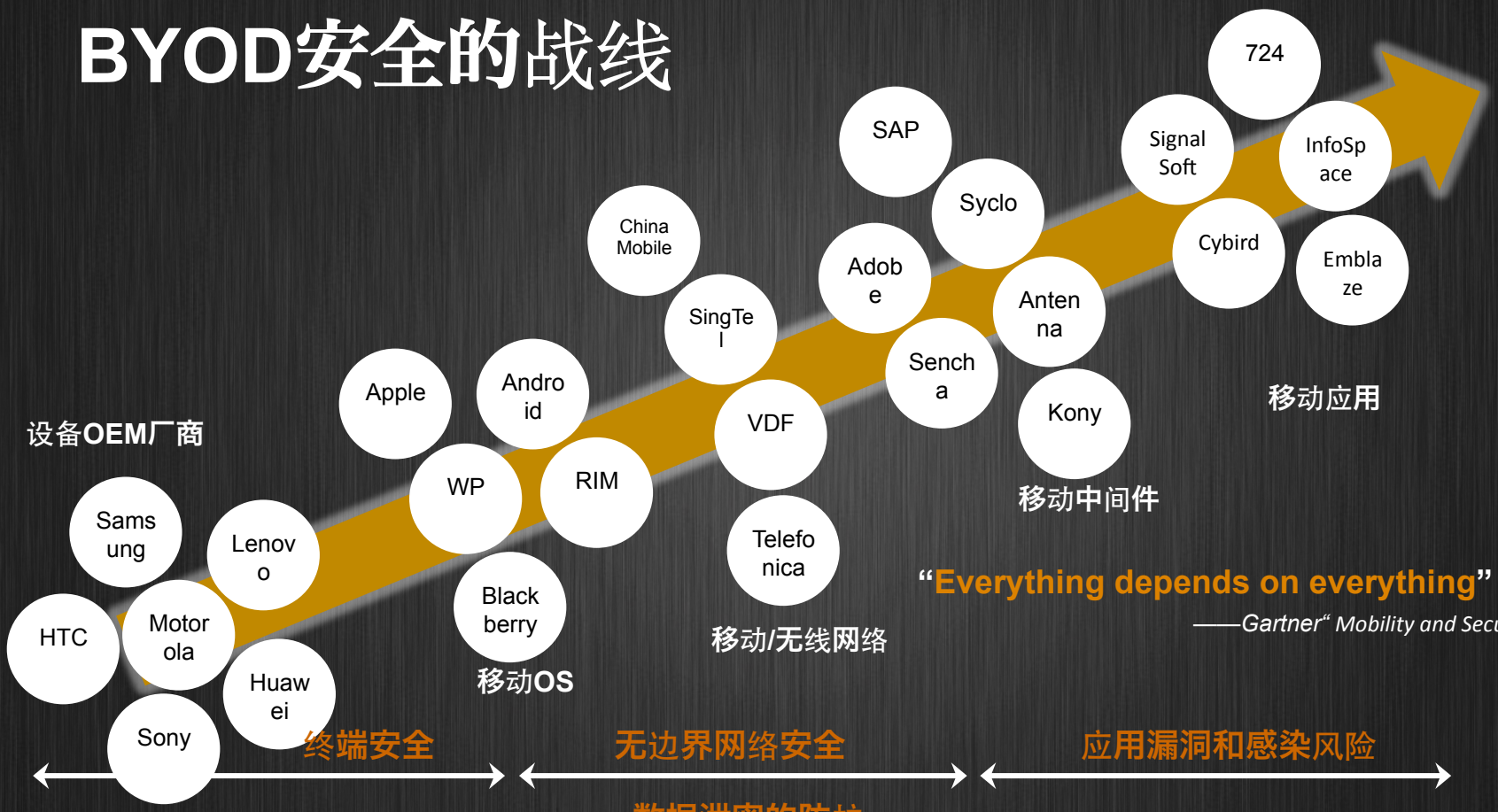
BYOD：Beyond your control?

BYOD之前CIO应该考虑的…

- 企业IT的边界模糊，如何确保企业安全策略的强制性？
- 企业业务环境和个人消费环境混合，如何有效的隔离个人娱乐和企业办公？
- 个人的无意行为引入病毒、间谍软件到企业环境，怎么防范以BYOD为跳板的外部威胁？

… …

BYOD安全的战线


724
SAP
Signal Soft
InfoSpace
Syclo
China Mobile
Cybird
Embla ze
Adobe
SingTel
Antenna
Apple
Android
Sencha
VDF
Kony
WP
RIM
Samsung
Lenovo
Telefonica
HTC
Motorola
Blackberry
Huawei
Sony
设备OEM厂商
移动OS
移动/无线网络
移动中间件
移动应用
“Everything depends on everything”
——Gartner“ Mobility and Security ”
终端安全
无边界网络安全
应用漏洞和感染风险
数据泄密的防护
统一管理

应对BYOD安全风险你需要做的

- Step1：构建一个安全的无边界网络，确保安全策略能够延伸到每个端点
- Step2：根据移动身份和环境，制定不同的安全策略
- Step3：确保必要的企业数据隔离和隐私保护机制
- Step4：对安装在设备上的应用进行安全鉴定，确保应用使用的安全

Step1：构建一个安全的无边界网络

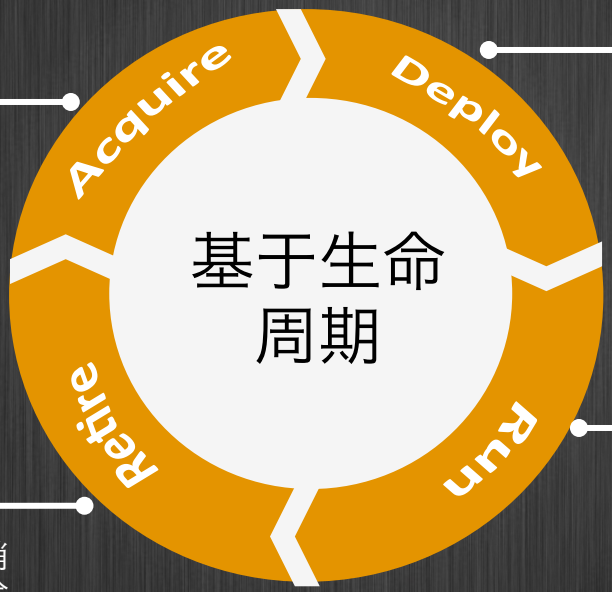
每个接入点和个人的载体

- 访问控制策略
- 数据防泄密策略
- 威胁防御技术
- 审计和遵从策略

Step2：实施差异化的安全策略

Who	内部固定员工	内部移动员工	合作方 / 访 客
What device	①PC用户策略	②公司标配机用户策略	③BYOD用户策略
策略	统一部署端点安全软件，访问内网所有资源	统一部署端点安全软件，通过VPN访问企业针对配给机分配的业务	按需部署端点安全软件，访问受限的内网资源
统一安全策略平台（基于4W+1H）			
Where	公司内 / 公司外	公司内 / 公司外	公司内 / 公司外
How	端点安全PC版：LAN、WLAN、VPN	端点安全移动版：WLAN、VPN	端点安全移动版：WLAN、VPN
What	公司所有应用：OA、IM、CRM、BPM、ERP、SCM、… …	公司大部份应用：OA、IM、CRM、BPM	公司受限的应用：OA、IM

Step2：确保您的策略得到强制执行



部署

- 应用分发、安装、配置更新
- 安全基础设施部署
- 安全策略配置和更新
- 资产统计

运行

运行

- 安全策略强制

安全策略强制

- 访问控制策略运行
- 通信链路加密
- 内容过滤等安全技术运行
- 应用升级、补丁管理
- 安全监控/资产审计和报告

回收

- 远程卸载、注销
- 数据回收和清除
- 设备重利用
- 硬件重配置、绑定
- 软件资产注销、重部署

获取

软件预置、安装

- 安全策略定义
- 合约管理：资产使用承诺等
- 资产发现、注册
- 初始化密码

- 安全策略定义
- 合约管理：资产使用承诺等
- 资产发现、注册
- 初始化密码

Step3：确保可靠的数据隔离和隐私保护

VDI

- 仅传输虚拟image文件
- 企业数据不保存本地
- 不能离线访问
- 实施成本高

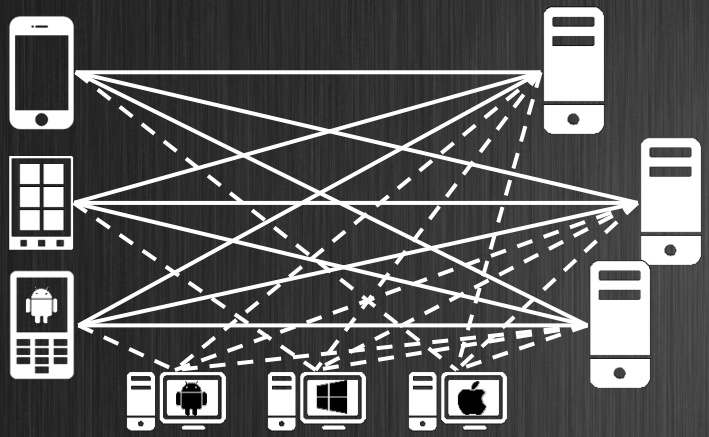
安全容器（沙箱）

- 数据操作行为限制、沙箱内数据加密
- 受应用限制
- 用户体验不高

移动OS虚拟化

- “终极”隔离
- 技术不成熟
- 缺少硬件支持
- 不支持多OS

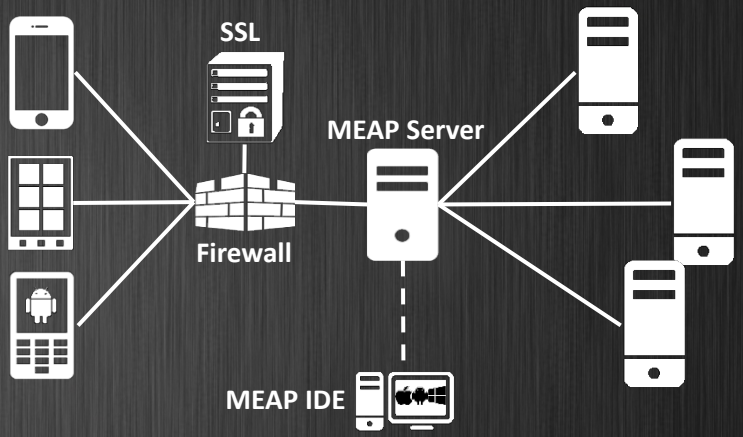
Step4： 寻找应用快速开发的方法，兼顾安全



高开发费用，应用上线周期长，维护难

终端网状访问业务，网络安全控制困难

安全特性实施和部署成本高，应用安全性差

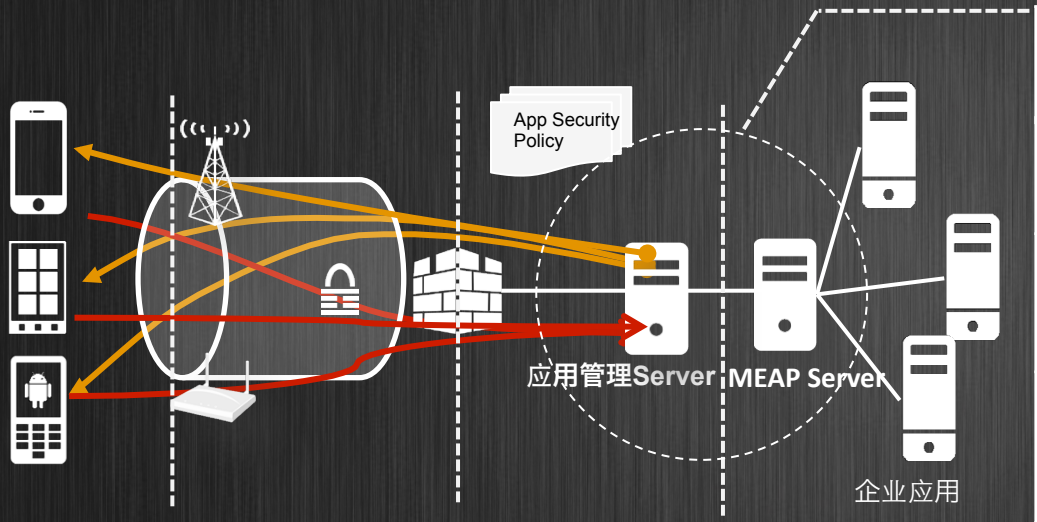


IDE，一次开发，跨平台发布，周期短，易维护

终端集中访问，应用集中适配，安全控制清晰

集成的SSL/SSO/MDM联动等SDK，高安全性

Step4：对应用进行安全鉴定



企业级App Store			
策略 / 应用类型	Required	Optional	Disallowed
In-house	OA	CRM	ERP
Recommend	msn	Gmail	

安全的应用鉴定、授权、发布和管理

安全的访问应用

推荐

1、构建一个安全的无边界网络，确保安全策略和技术可以随着网络延伸

2、从角色、支持设备、接入方式、开放应用等方面构建系统的BYOD策略，引入必要的技术确保差异化策略强制

3、选择适合的数据隔离技术，解决个人和企业应用、数据混合的根本矛盾

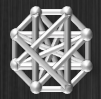
4、借助移动应用开发平台加速企业移动业务的迁移和价值，构建企业级App Store确保应用安全

BYOD的安全管理原则

Trusted：要有可信的设备

Role-based：能够基于企业角色进行安全防护

Enforced：各种策略必须能强制，不管移动到哪



Network be secure：网络应该是安全、无边界的

Dynamic：企业应用随需而动，实现服务化

BYOD趋势

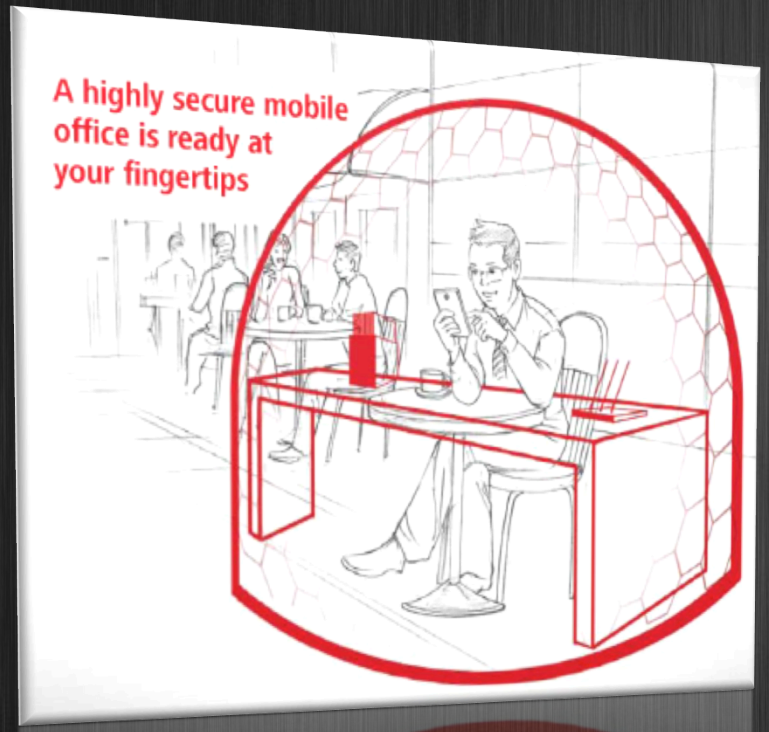
BYOD下的安全挑战和对策

华为移动办公实践分享

华为移动办公实践

- 华为全球有14.6万员工，每天有2.9万人使用移动终端访问企业内部应用，2.2万人使用移动即时消息服务，1.7万人使用移动Mail服务。
- **标配机策略：**
  1）统一预装的VPN和终端安全软件
  2）严格安全管控，统一互连网访问出口
  3）可广泛访问业务
- **BYOD策略：**
  1）安装VPN和终端安全软件，构建安全的无边网络
  2）个人数据与企业数据隔离
  3）有限的开放业务访问

ONE MORE THING…



华为安全移动办公发布会

2012年9月－10月， 敬请期待…

HUAWEI ENTERPRISE A BETTER WAY