
Virtual Mobile Infrastructure
企業資料不落地, BYOD的終極解決方案
iSecurity
The Hub of Security Innovations
sierraware

BYOD, 企業IT無可逃避的現實

- **95%的企業容許員工使用某種形式的自有個人設備** [1]
- **44%的大學畢業生希望進入支持BYOD的企業**[2]
- **容許BYOD的企業平均每年每人可提升產能 NT$33,000-110,000**[3]

1 *Cisco IBSG Horizons Study*
2 http://www.informationweek.com/mobile/6-risks-your-byod-policy-must-address/d/d-id/1107451?page_number=1
3 Dell Global BYOD Survey 2013

但是, BYOD的風險層出不窮

VDI技術不能解決BYOD的問題

VDI的缺點

頻寬需求高

不適用於3G網路

價格昂貴

Microsoft VDI或Citrix的軟硬體成本每人NT$35,000[1]

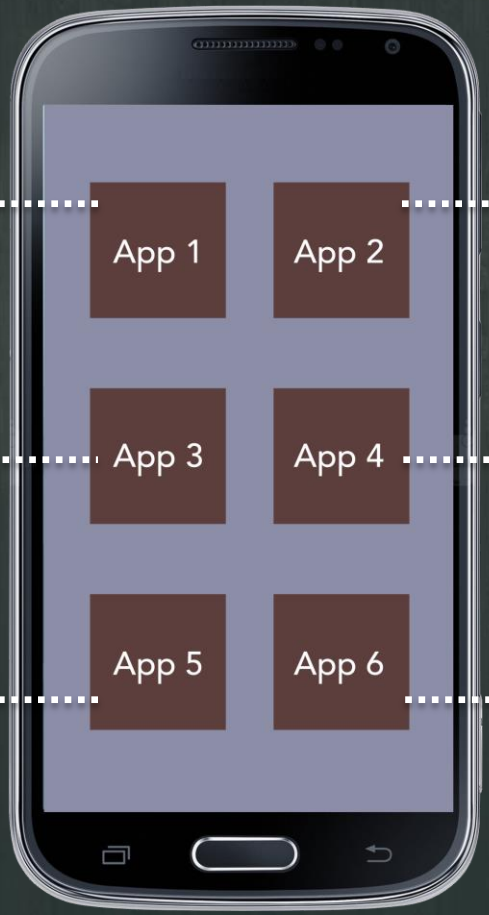
為Windows設計的界面

- 不適合觸控操作
- 無多媒體redirection
- 無法存取camera, printer, video, GPS

1 Microsoft Desktop OS NT$6,500/user, Citrix NT$10,500/user

手機OS與App的作業風險

無法符合個資法與PCI的要求



加密強度不足

薄弱的身分認證機制

未更新到最新版的App

個資儲存於非公司控管手機

無使用者存取記錄

未更新到最新版的OS

有一項新技術可以解決
前面描述的所有問題...

Virtual Mobile Infrastructure

Virtual Mobile Infrastructure (VMI)

VMI將企業App或full Mobile OS
Host在雲端或企業資料中心

員工使用手機或平板電腦內的
Thin Client App執行工作:

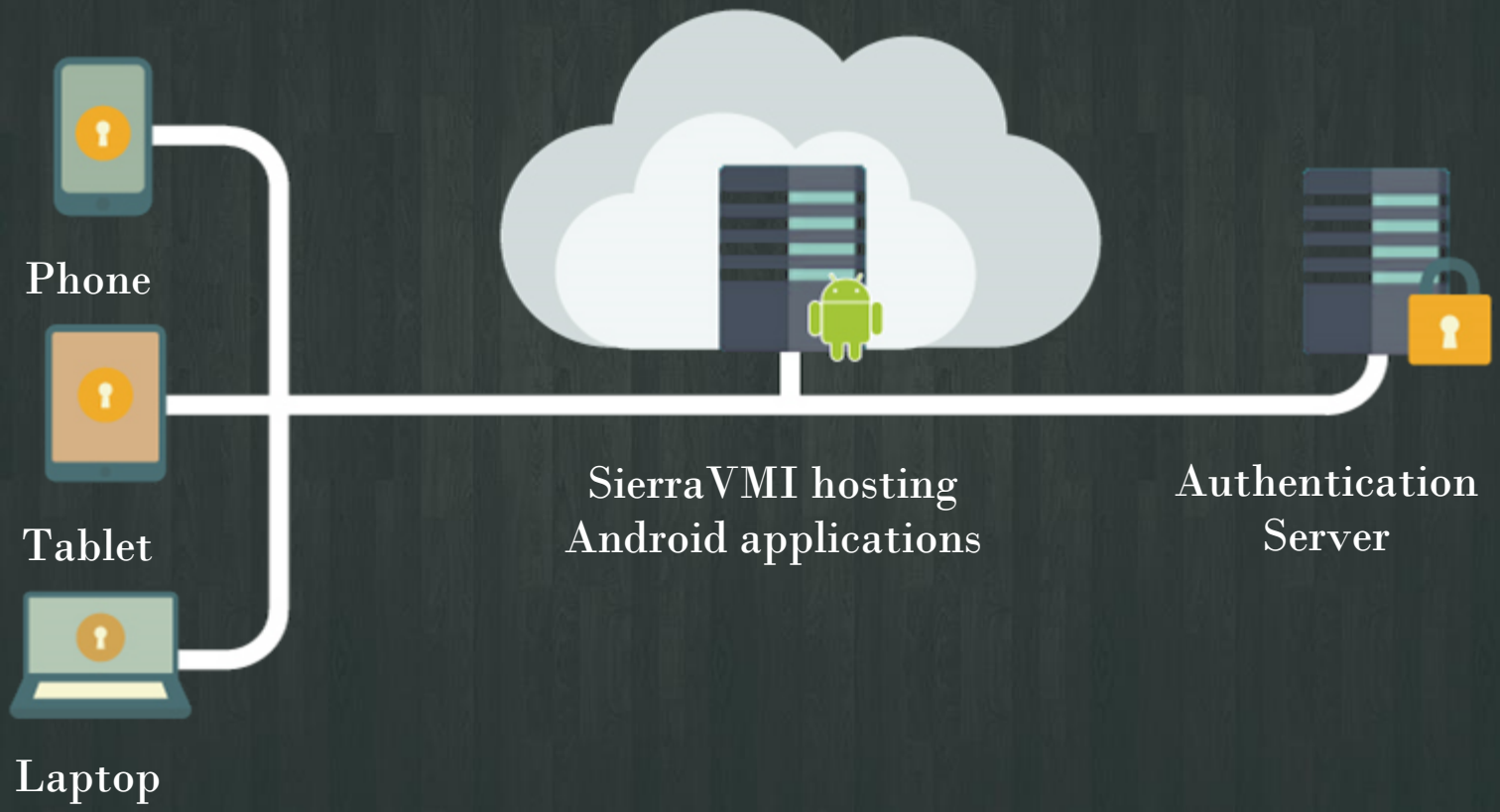
- Android, Apple iOS, Windows Phone
- 任何HTML 5-enabled設備



Centralized App Management:

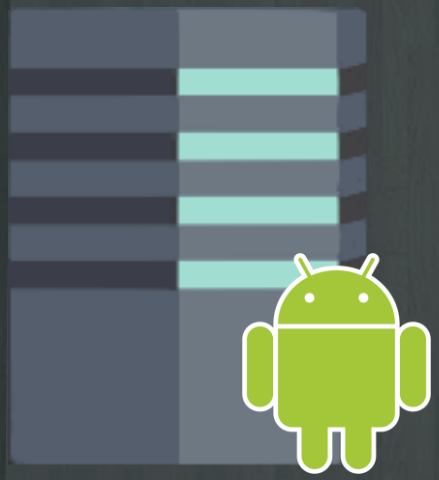
- 企業無需在員工設備上安裝與更新每一個App

SierraVMI示意圖



SierraVMI保護企業資料的安全

SierraVMI讓使用者無法
實際接觸企業資料‘



雙重認證機制

4096-bit ECDHE
加密機制

使用者

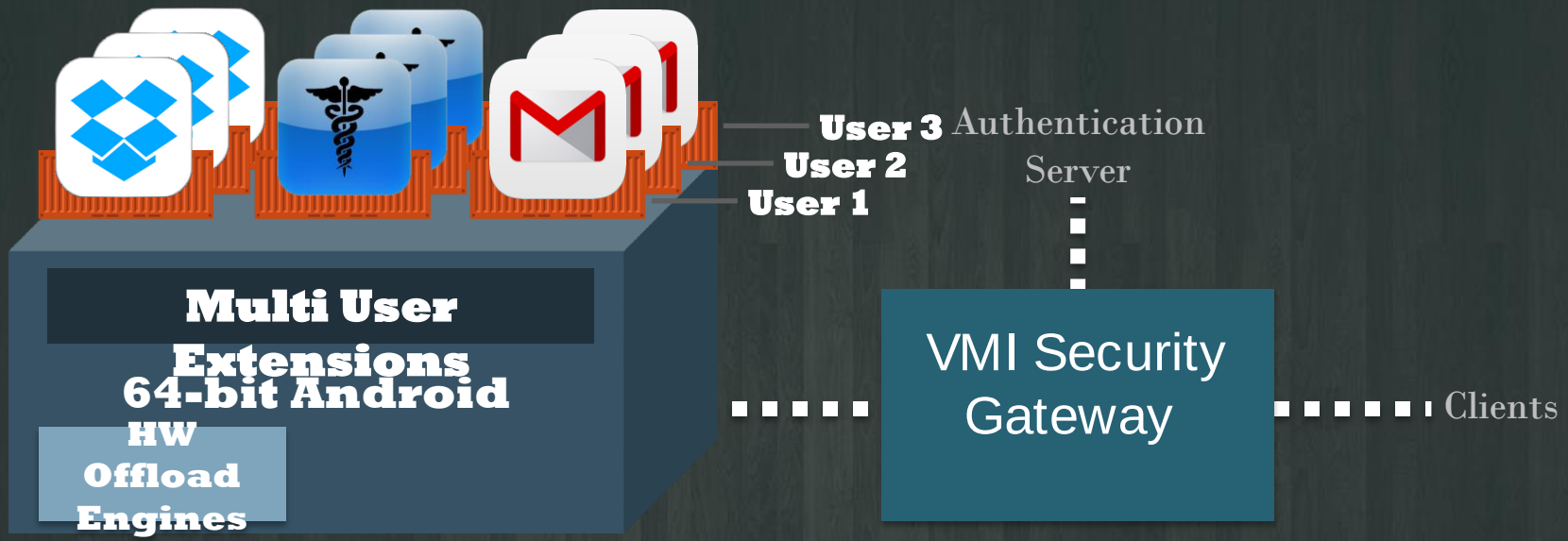
SierraVMI:

- 記錄使用者對企業App的存取
- 企業App與資料皆在資料中心, 永不落地手機
- IT再也無需煩惱App的安裝與更新

iSecurity
The Hub of Security Innovations

sierraware

架構1: Mobile App Virtualization



效益

- 使用密度高, 經濟性高
- User/App可共享系統資源, 如GPU
- 易於管理
- 無需添購昂貴的儲存設備

需考量因素

- 無法強制設定每一session可使用的硬體資源

架構2: Android LXC Container

效益

- 每一User可以自行安裝App, 適合開發測試人員
- Android版的desktop virtualization

需考量因素

- 使用密度低, 經濟性低

SierraVMI協助企業滿足 Mobile Security的五大核心需求

SierraVMI如何滿足mobile security的合規性需求

中央管控使用者對所有App的存取; 依據LDAP/AD群組訂定管控政策	視企業稽核需求, 可提供Detailed Log與Session Recording	有層次的存取控管; 並可於資料中心統一備份, 防範資料意外刪除問題	統一的多重身份認證機制	使用4096-bit加密與client cert認證機制

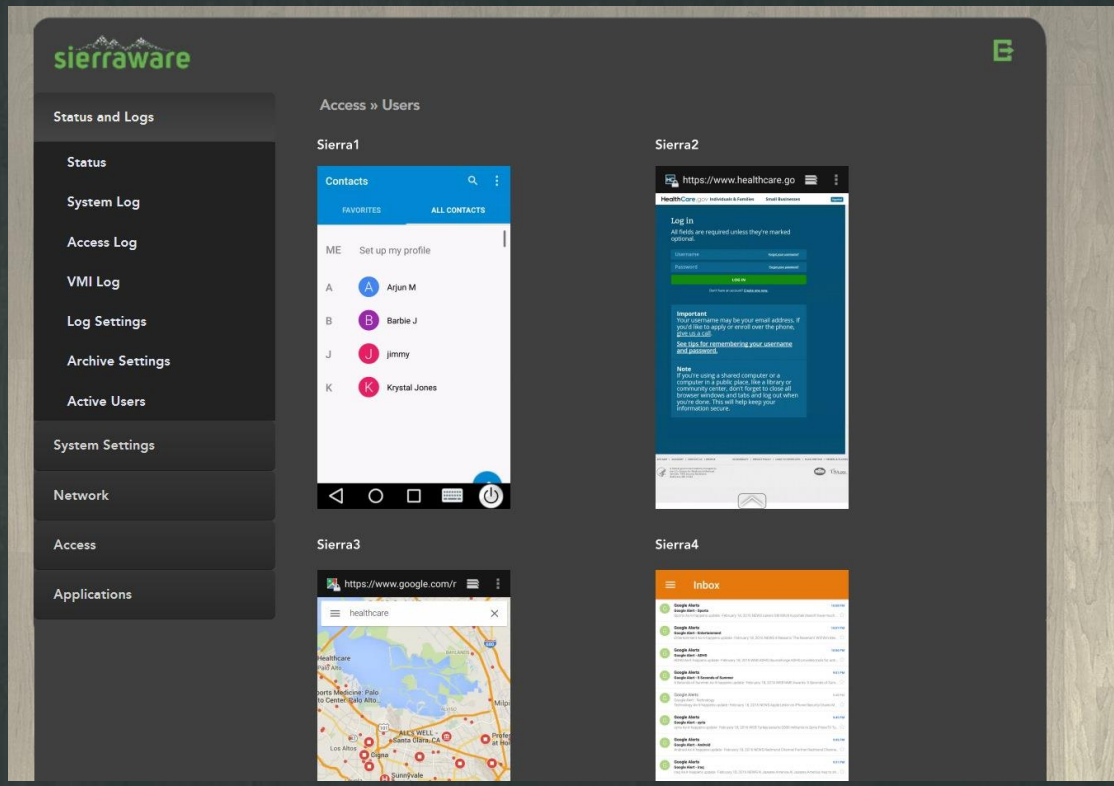
系統與使用者管理功能

- 系統管理儀表板
- 使用者行為的 log
- Geo-tracking

sierraware

對使用者行為的監控

- 記錄user sessions
- Admin最多可同時監看八個live sessions

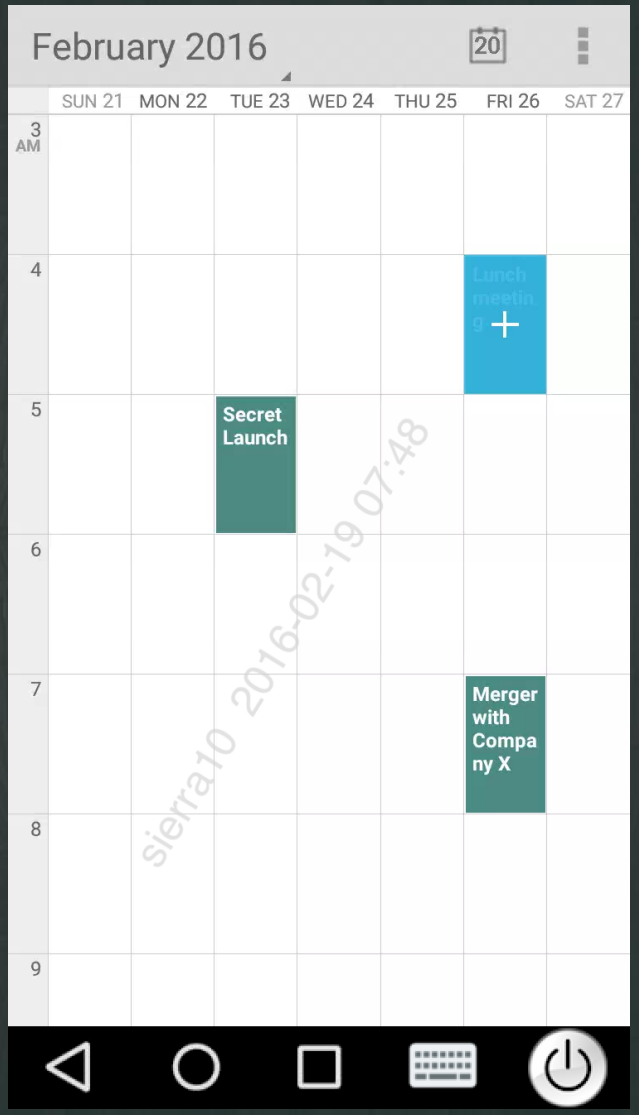


iSecurity
The Hub of Security Innovations

sierraware

防止資料外洩

- **浮水印功能**可有效降低user拍攝手機畫面的意圖
  - 可以無損效能方式, 對所有內容打浮水印(文件, 視頻, 相片)
- 反截屏技術(Anti-screen capture)
- 企業資料永不落地
  - 使用者無法copy and paste



VMI, 最安全的內容儲存與發佈機制

使用多媒體redirection技術, 安全分享敏感視頻

- 確保使用者無法下載任何檔案
- 所有內容皆可打浮水印

所有內容皆存放於企業資料中心, 而不是使用者的手機

高強度的認證機制

防止非法的存取:

- Client certificates
- One-time password (簡訊)
- 可根據手機所在地理位置, 限制使用者的存取
- 對暴力破解法(Brute Force Login)的防範

確保只有合法的使用者
才能使用企業App

Single Sign-on機制

Directory Services Integration

- 可與LDAP, Active Directory或SAML整合
- 使用者不需在使用每一企業App(email, calendar, contacts)時都需重新認證身份

IT Cost Reduction

- 自動化, 集中化提供使用者對所有企業App的存取
- 減少使用者因忘記密碼的IT helpdesk calls
- 簡化登入程序, 提升使用者滿意度

既方便又安全的Mobile App管理機制

- 集中儲存, 企業資料永不落地手機
  - 免除因設備遺失而導致的資料外洩風險t
- 中央patch management
  - 免除企業對BYOD手機軟硬體弱點的疑慮

Before VMI

- 企業倚靠使用者嫌惡的MDM產品執行Remote Wipe功能來防範手機端資料遺失
- 每一App都有不同的加密與認證機制
- 難以監控使用者對企業App的存取
- 遠端VPN進入企業網路的行為難以管理與監控
- 企業必須針對各種平台(iOS, Android, Windows Phone, Blackberry)開發多種版本的App

With VMI

- 企業資料永不落地手機, 無資料外洩之虞
- 所有App共享統一標準的多重認證, 加密與SSO機制
- 可視需要, 提供對特權使用者的logging與video recording
- 對遠端Mobile User提供多層次的管理與監控機制
- 企業僅需開發Android App, 透過VMI適用於所有平台

VMI Use Case範例

醫療

醫生使用平板電腦存取病歷與影像資料

金融

銀行AO/保險經紀使用手機/平板存取客戶資料

公用事業

抄表，遠端OPS/ICS/SCADA系統監控

交通事業

機動服務人員可協助旅客查詢航班與訂位

零售業

機動銷售人員可在賣場任何角落完成交易

電信/網路

Service providers提供value added hosting service

VMI Security Checklist

- 4096 Bit SSL
  - 防範意外與故意的資料外洩
- 保護使用者的隱私
- 協助企業合規: 個資法, PCI, SOX
- 安全的遠端存取
- 符合NIST SP 800-53與ISO/IEC 27002

iSecurity
The Hub of Security Innovations

sierraware

VMI的優勢

- 資料不落地，一個100%安全的BYOD企業工作空間
- 一個員工已經習慣使用的100%智慧手機作業環境
- 無需API，無需SDK，也不用App Wrapping，企業可以不受限制的自由選用任何Android Apps
- 一個Android App，所有平台共用，為企業節省App開發與維運城本
- 再也無須為使用者手機的管理而煩惱

現在，企業有了SierraVMI

所有的BYOD安全問題是不是全都解決了？

SierraVMI解決了幾乎所有的BYOD安全問題(翻攝自網路新聞圖片)

除了這個問題

還有這個問題

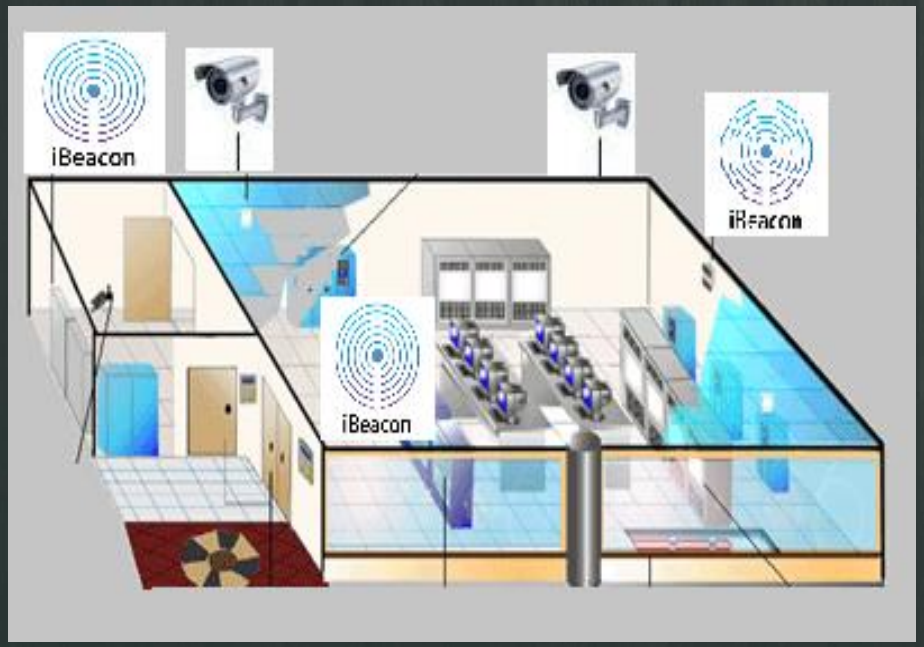
行動設備的相機如何管控？

- 行動設備拍照洩密事件頻傳
- 人員攜帶智慧型手機直入公司管制區域，已是公認的企業資安漏洞
- 但若全面禁用行動設備或破壞其相機功能，則會降低工作效率並引發員工反彈
- 坊間現有的GPS或WIFI based行動設備管控機制不但都有其技術上的限制，且永遠無法解決員工夾帶未受控手機進入管制區域的問題

Smart Curtain

- SmartCurtain專利的*iBeacon*微空間定位技術不但能讓企業有效解決行動設備相機問題，且能同時兼顧員工個人的權益

SmartCurtain 運用*iBeacon*技術執行資安管控



- 員工進入管制區域時自動關閉行動設備照相功能
- 所有App皆無法拍照
- 員工離開管制區時自動將所有功能恢復

SmartCurtain 適用於Android與iOS設備

SmartCurtain解決員工夾帶未受控手機進入管制區域的問題

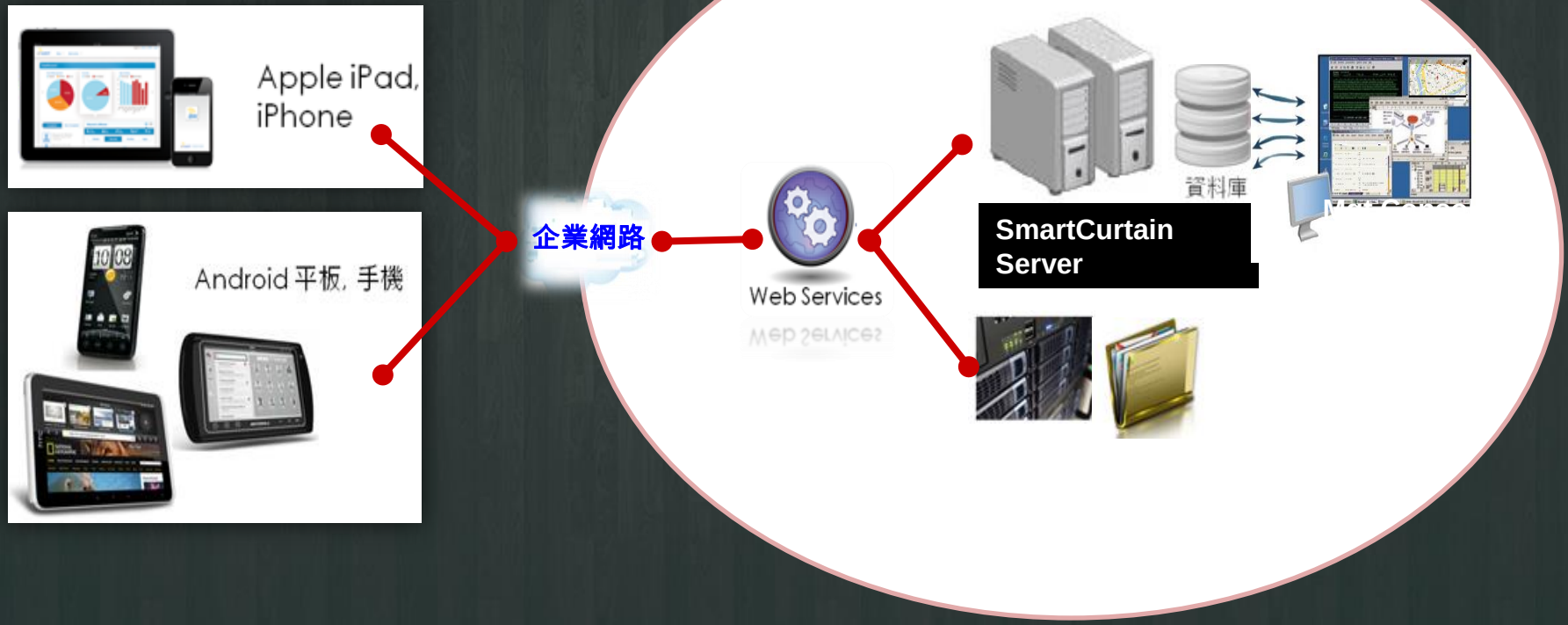
1. 管制區入口裝設金屬探測器(Metal Detector)
   →排除未被管制的手機
2. 管制區入口裝設*iBeacon*微型偵測模組
   →偵測手機是否被管制

Smart Curtain

未受管控前

納管後

SmartCurtain系統架構



iSecurity
The Hub of Security Innovations

SierraVMI + SmartCurtain

=

Total BYOD Security

sierraware