行動裝置多元化與管理

吳育贏
麟瑞科技股份有限公司
yuying_wu@ringline.com.tw

摘要

儘管組織內部對於行動裝置的應用，期許提升組織的效益，然而，實施行動裝置的管理需顧慮的層面廣泛，並非僅對員工開放設備即可，使得 IT 人員面臨困擾及壓力。

我們運用部署行動裝置資通安全管理、資安閘道、網路存取控制、桌面虛擬化或行動裝置上的〝傳輸加密〞等等解決方案，將相關的技術整合至組織內部架構，提供行動工作者容易地進入「辦公室」模式，並賦予行動裝置新的生命力，以嶄新的服務協助組織打造最佳效率與效益。

關鍵字：行動裝置、資通安全、資安閘道、網路存取控制、桌面虛擬化、傳輸加密

Abstract

We deploy information security management, information security gateway, network access control, desktop virtualization, or "transmission encryption" on mobile devices will be integrated into the organizational processes. We give a new service to help organizations create optimal efficiency and effectiveness.

Keyword: Mobile Devices, Information and Communication Security, Information Security Gateway, Network Access Control, Desktop Virtualization, Transmission encryption

1. 前言

過去二十年來，電腦幾乎主宰所有組織（機關、機構、大專院校、教學單位、學術單位、醫院、公司或企業、研究中心、其他附設機構……等，以下簡稱組織）的工作模式，隨著網路科技的進步，智慧型手機、平板裝置等行動裝置的應用，為 21 世紀人類的生活帶來革命性的創新與便利。

2. 行動裝置應用的趨勢

各位組織 IT 人員是否發現，近幾年辦公室有行動科技的革命悄悄在發生？越來越多同事把智慧型手機、平板裝置帶到工作場所，有些還連接到公司網路取用資料、處理公務。大多數的員工希望能使用一台智慧型手機、平板裝置或筆記型電腦，就可以同時處理工作的任務和個人的任務，而不願隨身攜帶公司的設備，造成員工攜帶自有裝置（Bring Your Own Device, BYOD）的趨勢。

智慧型手機與平板裝置等行動裝置由於攜帶方便、輕巧靈活，並可提供如：收發電子郵件、儲存文件、瀏覽簡報、遠端存取敏感或機密資料，甚至遠端直接存取組織內部的設備或伺服器等功能特性（圖一），有助提高行動辦公環境的生產力與效率。

圖一 行動科技的革命悄悄在發生

新世代的行動服務發展除了行動裝置產品本身技術越來越成熟外，另一個必須被提到的重要因素，就是先進國家在政府主導下逐步規劃其下世代的行動服務發展藍圖。以美日韓而言，均已提出至 2020 年之行動通信服務發展規劃，歐盟則成立啟動 2020 新世代生活計畫聯盟進行相關服務研發；目前，台灣提供無線網路的辦公環境、免費 Wi-Fi 服務的公共場所比例亦大幅增加，而電信業者建置的行動網路連線（如 Wi-Fi、3G or 4G）也成為商業人士用來進行商業性溝通的重要角色。

國際研究暨顧問機構 Gartner（註 1）曾指出至 2018 年，裝置、運算形式、使用者情境以及互動模式將日趨多元化。員工攜帶自有裝置計畫促成行動工作人口規模呈現加倍、甚至三倍發展至始料未及的結果。綜觀未來，具高度行動力的協同合作無疑是組織致勝關鍵，彈性的工作環境能有效提高個人生產力，進而強化組織競爭力，組織應積極思考如何運用行動裝置，打造高度彈性且安全的溝通模式與工作環境。

3. 如何應對行動裝置多元化

為加強行動裝置的資安防護，避免可能的風險與危害，提供行動裝置資通安全防護，組織 IT 人員可考慮由以下的五個面向進行管控與部署。

3.1. 組織應考量部署行動裝置資通安全管理解決方案

行動裝置到處可購得，這些電子產品，有助提高行動辦公環境的生產力與效率，但同時也帶來新的資安威脅。為能顧及個資法，落實個人資料的保護及提昇組織的服務品質，應考量建構行動裝置資通安全管理。

行動裝置資通安全管理就如同個人電腦系統的資安管理，任何有效的技術防禦措施仍須搭配可行的管理規定並落實執行，才能減少資安威脅的持續存在。

為了管理這一新興技術與趨勢，組織還應部署具備中央控管的解決方案，以大幅減輕 IT 人員的工作負荷及確保行動辦公環境中所有終端裝置的安全。

3.2. 組織應考量部署資安閘道解決方案

如網路防火牆、新世代資訊防護閘道或網路入侵防禦系統（IPS）並將它們配置為控制和監測所有設備的進出流量，尤其是特定敏感或機密資料的流量，組織更應嚴格監控。

3.3. 組織應考量部署網路存取控制(Network Access Control, NAC）解決方案

對於透過無線網路連線的行動裝置使用者，不論其是使用公司管理或是攜帶自有裝置，只要連線進入公司，都應該受到公司安全政策的檢驗，阻斷不信任的設備，如同保護 LAN 的使用者一般，達到管制的目的。NAC 可以判定公司管理或是攜帶自有裝置的各種狀況，如：是否有安裝個人防火牆、作業系統補丁、病毒碼更新之狀態，以及是否有組織指定的軟體存在於註冊機碼等各種情形可以控制存取裝置和其他未受管理之終端，確保它們只能有限度的存取組織資源，避免其對組織資安的影響。

3.4. 組織應考量部署桌面虛擬化（Virtual Desktop Infrastructure, VDI）解決方案

員工擁有的智慧型手機或平板裝置可能同時用於個人訪問和業務應用。基於雲端的檔案共用和存儲服務對於個人資料很方便，但可能是洩露組織機密資料的潛在因子，IT 人員必須制定用於保護業務資料的策略。無論是公司管理或是員工攜帶自有裝置，需在行動裝置建立一個安全業務分區，透過桌面虛擬化（VDI）允許對敏感或機密資料進行讀取，而不將資料直接存儲於行動裝置。這樣的解決方案也能為雲端部署的安全性，提供單一、具成本效益的架構，這樣員工可以通過行動裝置存取組織內部的應用程式和資訊，但同時把敏感或機密資料仍保留在組織內部的伺服器。

3.5. 組織應考量部署行動裝置的〝資料保護〞或〝傳輸加密〞解決方案

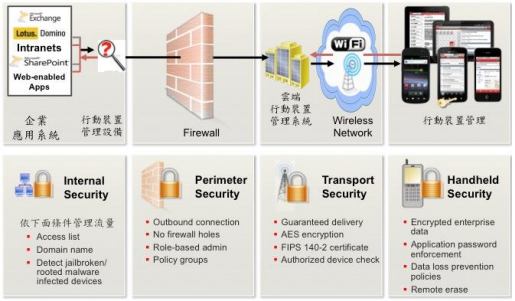
要求員工對公司管理或是攜帶自有裝置針對存儲訊息要進行保護，以便在行動裝置遺失或遭竊時，避免敏感或機密資料落入有心人士之手。另外，行動工作者連接到網路不僅是為了讀取組織內部的資料，也是希望可以與其他組織內部人員進行協作。就像在傳統工作場所一樣，行動工作者可透過傳輸加密來進行語音、視頻或會議服務，加密的傳輸可進一步確保資料不外洩。

4. 行動裝置多元化的管理

IT 人員也別因為恐慌而一昧圍堵行動裝置的多元化應用。行動裝置本身不是問題，IT 人員需要關注的是行動裝置存取組織內部敏感或機密資料的過程，尤其是針對裝置的身分識別、網路存取等級和行動應用系統的管理措施；本公司提供多元的解決方案：

4.1. 部署行動裝置資通安全管理解決方案

思科網路設備可以配合行動裝置管理系統如：MobileIron, Good Technology, AirWatch, Sophos 提供多種行動裝置系統平台的管理（圖二）。



圖二 行動裝置在資安上的縱深防禦

針對行動裝置系統平台的管理與設計，至少需考量以下的功能：

- 提供單一管理平台可集中管控各式各樣的行動裝置，包含 Apple iOS、Android、Samsung SAFE、BlackBerry、Windows Phone & Symbian（可視組織的需求，確認是否需要管理這麼多類型的行動裝置）。

- 提供行動裝置管理原則，並可管理以下項目：a. 強制設定鎖定密碼與複雜度原則、b. 強制設定密碼容錯次數與自動抹除資料、c. 管制行動裝置的照相功能、d. 管制行動裝置的原生應用程式，例如：應用程式線上商店功能、e. 管理行動裝置的應用程式清單，具備控制行動裝置各項功能或應用程式的使用，如任意安裝軟

體等，防止資料洩露及中毒受駭的資安風險。

- 提供安全規範檢查原則，並可檢查以下項目：a. 偵測越獄（Apple iOS）或取得 ROOT 權限（Android）的行為、b. 行動裝置作業系統版本的變更、c. 更換 SIM（Subscriber Identity Module）卡。

- 管理人員可透過管理主控台對行動裝置執行以下強制措施：a. 遠端鎖定、b. 遠端抹除資料、c. 重設鎖定密碼。

- 提供應用程式部署機制，應用程式來源需包含：a. 應用程式線上商店（例如：Apple App Store 與 Google Play）、b. 自行開發的客製應用程式。

4.2. 部署資安閘道解決方案

市面上有許許多多的網路防火牆、新世代資訊防護閘道就沒有在此一一說明，僅就次世代網路入侵防禦系統（IPS）及視訊通信閘道稍做說明。

- 次世代網路入侵防禦系統：由於 BYOD 的盛行，不少人使用軟體的比例，已經從電腦轉移到行動裝置。而次世代 IPS 針對這部分，讓 IPS 能夠控管行動裝置的瀏覽器、通訊 App 如 Facebook、Line、微信等而這些都非原本 IPS 所具備的能力(圖三)。針對次世代 IPS 的管理，至少需考量以下的功能：a. IPS 虛擬化，以便保護虛擬環境的網路存取、b. 因應已知弱點資訊，自動補強設備的網路防禦規則、c. 防護 Botnet 及 APT 等進階攻擊，提升設備應變能力、d. Layer 7 控管不再侷限電腦軟體，需可控管行動裝置 App。

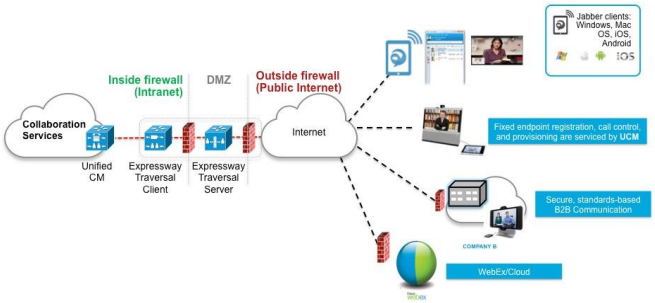
圖三 原本 IPS 無法完整掌控所有設備及行動裝置

- Sourcefire 新世代入侵防禦系統，顛覆我們對 IPS 的概念與印象，以獨家的 FireSIGHT（被動探索）技術分析通過 Sourcefire IPS 的封包，以獲得最即時的內容，包含網路設備、作業系統、應用程式、行動裝置及網路流量等資訊，IT 管理人員可透過設備，查詢被攻擊主機的作業系統、執行的端點程式、對外開放的服務等資訊，這都能協助 IT 管理人員在攻擊事件後，調查事件來源，及針對弱點增加防禦規則，也就是說，它能讓 IT 管理人員隨時掌握組織內部網路的一舉一動(圖四)，然後再根據這些資訊，給予 IT 管理人員最佳的防禦建議(或可自動調校規則設定)。這樣的做法，徹底解決傳統入侵防禦系統的空窗期、無法即時回應等問題。

圖四 隨時掌握網路的一舉一動

- 更特別的是，Sourcefire IPS 還能監控是否有違反公司安全政策的事件，例如員工違規安裝不合法應用程式、或是攜帶自有裝置連線至組織內部等等違反公司的安全政策，都會立即通報 IT 管理人員。

- 視訊通信閘道：建置 Cisco Expressway 閘道器（註 2）支持行動工作者或分散式團隊更高效地開展工作，不但提供各種行動裝置的通訊控管，提供「身分辨識」功能，讓用戶在不用建立安全的遠端網路存取（如 VPN）的情況下，也能擁有高度安全的通訊環境（圖五），舉例來說，行動裝置無須透過安全的遠端網路存取（如 VPN），便可將視訊系統功能延伸至 IT 認可的裝置，如平板裝置（iPad）、筆記型電腦（Windows、Mac OS 作業系統）。



圖五 可「防火牆穿越」、「身分辨識」的行動裝置通訊控管

4.3. 部署網路存取控制（Network Access Control, NAC）解決方案

未來的 NAC 方案，其控制重點在於如何維持一貫的網路控管政策，並且也能允許攜帶自有裝置經由身分與設備驗證之後，在組織中能夠合理的應

用。

以下將是下一代 NAC 因應攜帶自有裝置的挑戰，所應具有的功能或特色：

- 網路身分驗證：偵測與區分線上設備屬性，如找出非網域設備，未植入 NAC 管理程式的設備或使用固定 IP 之設備，管理其使用。

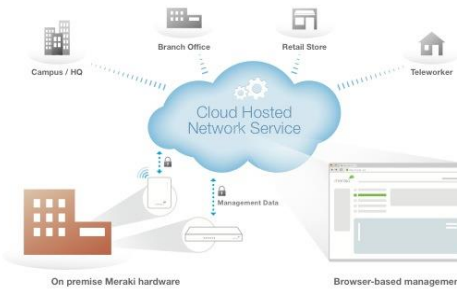
- 線上設備連線資訊檢視：檢查終端設備作業系統的安全性更新，IP、MAC 更動或不當程式執行。

- 保護組織敏感或機密資料：確保終端設備在網路上的存取行為的合法性，若檢查不符合，即強制矯正,如透過 Cisco ACL 來限制存取網路。

- 延長設備投資效益：與組織既有設備（VPN, F/W, IP……）搭配或互補以延長現有設備之使用效益及提高組織的資安嚴謹度。

- 降低管理成本：強化組織內部管理機制及訪客存取管理，以利提升組織網路安全性，降低 IT 人員工作負載。

針對組織辦公地點較為分散或無專屬負責這個領域的 IT 人員,建議採用 Meraki 雲端無線網路架構，以利因應攜帶自有裝置的挑戰（圖六）:



圖六 分散式運作・集中式控管

- 網路身分驗證：無線網路安全認證可支援 Mac address 黑白名單、802.1x、內部或外部 Radius 伺服器及 Microsoft Active Directory。

- 線上設備連線資訊檢視：a. 與 Google 地圖整合：顯示無線網路基地台所在位置，可依照需求，自行設定顯示方式，如：地圖、衛星圖、混合地形圖、地形圖及樓層圖等、b. 無線網路管控：針對不同的作業系統進行管控，如智慧型手機平板裝置（Android 平台）或平板裝置（iPad）進行管控（圖七）。

圖七 輕鬆管理各式各樣的行動裝置

- 保護組織敏感或機密資料：a.訪客無線管理：訪客使用之無線網路之規劃，並能客製化其認證畫面及訪客可存取之網路區域，以強化無線網路管理、b. 防毒檢測機制:為強化訪客管理，無線網路具備 NAC 檢測機制，訪客在開始使用無線網路前，能夠檢測訪客電腦之防毒軟體。

- 延長設備投資效益：與組織既有資安閘道設備（網路防火牆或網路入侵防禦系統……)搭配，如限制用戶使用色情網站、免費 Email、社交網站、照片分享網站、P2P、病毒更新、線上檔案儲存、線上備份及電腦遊戲等應用程式，以利延長現有設備之使用效益及提高組織的資安要求。

- 降低管理成本：提供全 Web 化管理介面，無需使用複雜且難記之命令模式（CLI）操作方式，隨時隨地掌握無線網路之狀態。

4.4. 部署桌面虛擬化解決方案

為了方便組織佈署雲端運算，思科行動裝置解決方案可配合虛擬化桌面領導廠商如:Citrix、VMware、Wyse 之應用，方便組織建構資料不落地、機密不外洩且易於管理的行動辦公室（圖八）。

圖八 建構資料不落地、機密不外洩的行動辦公室

以下針對 VMware Horizon View Client 因應攜帶自有裝置的挑戰，所應具有的功能或特色：

- 雲端存取:與傳統 PC 及筆記型電腦不同的是，Horizon View 桌面位於雲端，不用固定在實體電腦上執行。從任一位置，使用智慧型手機或

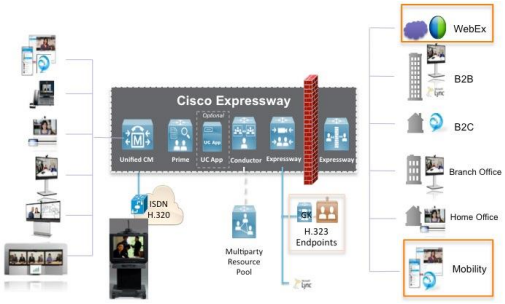
平板裝置，在安裝 Windows 的 Horizon View 虛擬桌面進行作業。

- 使用者體驗：針對行動裝置而言，Horizon View Client 支援原生智慧型手機（如 iPhone）或平板裝置（如 iPad）手勢，可快速和輕鬆瀏覽桌面。針對 Windows 而言，全螢幕觸控功能讓您可在螢幕任一處觸碰，在 Windows 虛擬桌面上移動滑鼠指標。
- 簡易連線：iOS 版 or Android 版 Horizon View Client 緊密與 VMware Horizon View 整合，可簡便進行設定並輕鬆進行連線。從最近的桌面清單選取，快速重新連線至所需的辦公環境。

- 資料安全無虞：Horizon View 以集中式服務方式來提供並管理桌面、應用程式及資料，藉此提高資料安全的控管能力。

4.5. 部署行動裝置的〝傳輸加密〞解決方案

為了滿足行動工作者進行語音、視頻或會議服務，可透過思科提供的 Jabber（註 3）或 WebEx（註 4)實現移動終端的語音、視頻、即時簡訊(IM)、人員狀態等協作體驗，而且在任何地點，無論是在家裡、飯店、機場、醫院或其他公共場所都可隨時接入，隨時溝通（圖九)。



圖九 行動工作者可隨時接入，隨時溝通

以下針對思科 Jabber 因應攜帶自有裝置的挑戰，所應具有的功能或特色：

- 快速通訊：智慧型手機（如 iPhone）或平板裝置（如 iPad）透過 Jabber 提供狀態資訊服務可以減少通信的延遲，以方便地查看聯絡人是否有空並能與他們做訊息的溝通。

- 整合通訊服務延伸至行動工作者：從一對一的對話可立即擴展到群組聊天、多方的音訊或網真會議，以大幅提升組織效能。

- 單一電話號碼進行行動通訊連結：直接與微軟 Office、Outlook 或 SharePoint 做協同合作並查看連絡人是否有空，只要按一下就能進行 IM 或通訊。

- 較低的行動成本：Cisco Jabber 可做網路語音通話（VoIP)、視頻或會議的功能，以利組織降低差旅費及電話費用。

- 雲端存取：透過自建(on-premises)的私有雲，在任何有行動網路連線的地點都可隨時接入，隨時溝通。

5. 結語

儘管組織內部對於行動裝置的應用，期許提升組織的效益，然而，實施行動裝置的管理需顧慮的層面廣泛，並非僅對員工開放設備即可，使得IT人員面臨困擾及壓力。

我們運用部署行動裝置資通安全管理、資安閘道、網路存取控制、桌面虛擬化或行動裝置上的〝傳輸加密〞等等解決方案，將相關的技術整合至組織內部架構，提供行動工作者容易地進入「辦公室」模式，並賦予行動裝置新的生命力，以嶄新的服務協助組織打造最佳效率與效益。

參考文件

Cisco英文官方網站 http://www.cisco.com/
Cisco中文官方網站 http://www.cisco.com/web/TW/index.html
CIO IT經理人網站 http://www.cio.com.tw/
資安人科技網站 http://www.informationsecurity.com.tw/main/index.aspx
今日新聞網站 http://mag.nownews.com/
數位時代網站 http://www.bnext.com.tw/
iThome電腦報網站 http://www.ithome.com.tw/
VMware網站 http://www.vmware.com/tw
逸盈科技網站 http://www.netfos.com.tw/
亞太信息網站 http://www.infosource.com.tw/
達友科技網站 http://www.docutek.com.tw
維基百科網站 http://zh.wikipedia.org/zh-tw/

註1：高德納（英語：Gartner）是全球最具權威的IT研究與顧問諮詢公司，成立於1979年，總部設在美國康涅狄克州史丹福。其研究範圍覆蓋全部IT產業，就IT的研究、發展、評估、應用、市場等領域，為客戶提供客觀、公正的論證報告及市場調研報告。

註2：Cisco Expressway閘道器：建立在Cisco協作的邊緣架構，使組織外部的用戶安全地連接到內部業務的協作工具。新的閘道器無需VPN連接，用戶可以直接加入。

註3：Jabber：Cisco Jabber是一個軟體電話可做視

訊和桌面共享功能。簡述：透過此一整合通訊軟體展開協同合作,可以輕鬆存取即時狀態、即時訊息、語音與視訊、語音訊息、桌面共享與會議等功能。

註4：WebEx：Cisco WebEx以網路瀏覽器（如使用任一個Firefox, Internet Explorer, Chrome, Safari等瀏覽器皆可正常）將桌面共享功能與電話會議和影音結合，免除傳統網路視訊會議所需各項設備的設定。

（作者現任職於麟瑞科技）