IBM Security
創新思維領導白皮書

行動化您的公司內容及應用程式

為企業啟用簡單和受保護的行動協同作業

IBM

新時代的行動策略

問：您是否有穩健強大的行動策略？

答：行動策略？您是指，我們的員工能不能在其行動裝置上存取電子郵件？這樣的話，當然有了。

如果這是您的答案，您並不是唯一一家這麼想的公司。許多公司仍然仰賴電子郵件做為讓員工與辦公室外部人員聯絡的「精選應用程式」。即使只是在幾年前，這也是一項巨大的勝利。然而，事實上，檢查電子郵件和回覆辦公室外部人員並不只是像移開障礙物、一路移動東西並保持外觀這樣的「工作」而已。在今日世界中，行動協同作業有巨大潛能可激發真正的生產力，並以幾乎即時的速度加速實際作業，但許多公司淺嚐即止，而忽略了採納、規劃和部署穩健強大的行動策略，以善用行動力的能力來簡單且受保護地存取商業資源。

在此文件中，我們會討論如何將持續監控套用至筆記型電腦、桌上型電腦和其他終端裝置。

在此白皮書中，您會學習如何：

- 透過受保護的行動方式存取公司資料，而不需要裝置上的 VPN
- 賦予 SharePoint、Windows 檔案共用及所有內部網站行動能力
- 利用穩健的安全性政策和 DLP 控制項來保護敏感性的企業資料
- 提供行動存取權，而不需要變更網路或防火牆的安全性組態
- 可讓使用者透過個人裝置隨時隨地協同作業

閱讀內容以深入瞭解您如何讓員工存取防火牆後方的資源，同時還能利用授權、加密和容器化原則來保護資料。

簡單且安全地存取

以下是一個簡單的挑戰：打造安全無虞的房屋，保護所有無價珍寶。要如何達到這個目的？您可以打造沒有任何門窗的房屋，完全沒有出入口。這可能安全無虞，但在實際生活方面並不是非常實用。或者，您可以打造具有精密鎖和保全系統之門窗的房屋來保護貴重物品，而且能有效地擁有相同等級的安全性，但仍然可以進出、迎接訪客和享受新鮮空氣，而不需要承擔損失貴重物品的風險。

您的行動策略可能就像是沒有門窗的房屋。或是，可能像是有門窗卻沒有上鎖的房屋。您要負責保護公司內容，但您也要提供這些內容給使用者，讓他們發揮生產力。從客戶聯絡人名單到患者資料、財務資訊到人資檔案、從公司應用程式到董事會記錄，全體員工需要存取的資訊每天日益增加，封鎖存取權不再是可行的選項。您需要一些門窗及保全系統，才能協助確保有權限的人才能進入。

如果使用者攜帶個人的智慧型手機或平板電腦到工作場所，並將業務聯絡人資料下載到裝置，該怎麼辦？如果他們將專屬財務報表以電子郵件寄送到住家電子郵件地址，以便能在子女入睡後處理公務，該怎麼辦？那廠商呢？您想要共用內容和應用程式，如此就能更有效率地協同作業，但專案結束之後該怎麼辦？

這些情況每天都在發生。除非您能加速執行更安全、可靠且簡單的方法，讓人們取得所需的內容，否則人們會想辦法取得自己需要的資訊，而讓公司資訊陷於危險之中。

內容考量

企業內容會儲存在公司網路上的 Windows 檔案共用、SharePoint、內部網站和 Web 應用程式等位置中。人們需要用來與同事、合作夥伴和客戶協同合作以完成工作的資訊是困在內部磁碟機和資料儲存區、知識庫、內部維基百科、ERP、SCM、HRM、CRM 及其他管理系統或程序中。

所以，問題變成是您如何將這當成基礎，為需要即時存取權的現代行動員工提供資訊？而且很多時候都是透過不屬於公司財產的裝置進行存取。

當您保護自己的資料和內部網路、檔案共用以及裝載資料的其他系統時，您可能需要考慮下列事項，將其列入您的行動策略中。某些看似明顯，但值得留意。

1. 內容必須可讓使用者依需要透過推播或提取的方式加以存取。
2. 根據路徑位置及識別， 每個使用者都必須只擁有所需內容的存取權。
3. 經過一段時間後資料必須可以跨裝置進行更新和同步。
4. 對使用者而言，存取資料的程序必須不會很繁瑣。
5. 維持安全性不能所費不貲，雖然這是一項大投資。
6. 對 IT 而言，維持安全性不能是曠日費時的工作。
7. 傳輸中的資料必須加密和受到保護。
8. 未經授權，資料不得離開組織。
9. 在應用程式中建立和儲存的資料必須受到保護。
10. 因為個人裝置並非由組織所擁有，您可以控制的項目有所限制

任何聯邦網路安全性立法的其中一個最重要目標是，必須要讓防護者能夠在攻擊者有所動作時立即快速採取行動來保護系統。

目前的技術

讓我們看看今日使用的技術，啟用安全性及生產力時會發生某些固有問題。

電子郵件

電子郵件是進行協同作業的精選應用程式，但只是眾多工具中的其中一個。

它的設計並非適用於協同作業。電子郵件支援一對一或一對多通訊，而不是使用者真正發揮生產力所需的多對多互動。這樣會造成在原本應該合作的群組之間發展出獨立的管理系統。

以電子郵件傳送的資訊很容易就會過時，人們收到了一個試算表然後就持續使用這個試算表，而不知道其中的內容已經被某些更新內容取代了。

最大的問題在於資料可能被剪下、貼上並轉寄到您不想要寄送的地方。

VPN

使用 VPN 登入是在防火牆後方提供存取權的常見選擇。

可惜的是，強制使用者登入以存取內容會導致使用者體驗降級。如果讓您選擇是要取得比較難存取的全新內容，或是要易於取得的過時內容 (以電子郵件附件的老方法寄送)，人們可能會選擇較簡單的方法。

VPN 需要每個裝置一個授權，所以成本可能隨時間而倍增。此外，證據顯示裝置 VPN 可能加速裝置電池的耗電量。

因為行動裝置會使用無線技術來進行連線，所以您需要加密。但是，漫遊時，存取發生問題。在一般情況下，當使用者在存取點之間漫遊時，仰賴較高等級加密的解決方案比較有可能中斷。幸運的是，某些解決方案可以解決該問題。

桌上型電腦虛擬化

某些應用程式可讓您在行動裝置上顯示桌上型電腦的桌面。可從桌上型電腦存取的所有項目也都能從您的智慧型手機或平板電腦取得。但是，這樣的費用通常所費不貲，而且使用者體驗可能不是很好。使用這個方法，可用性及效能與網路連線能力息息相關。此外，螢幕尺寸及解析度問題則帶來另一項挑戰，特別是在具有小螢幕和工作區的智慧型手機上。針對桌上型電腦環境最佳化的應用程式可透過桌面虛擬化而在行動裝置上存取，但那不代表這些一定適合使用。

另一項 IT 需要考量的事項是，伺服器和網路資源必須要能夠支援同時連線至其網路的許多裝置。

協力廠商檔案共用

協力廠商檔案共用可讓您將資料放在雲端中保持可用。其中一個大問題是您沒有任何控制能力，內容可能會被傳送給任何人、被任何人存取，而且您可能會有版本控制問題。

也有使用者體驗問題。使用者不喜歡只是為了存取所需內容，而被強迫學習新軟體，另一個考量因素是訓練使用者使用內容所花費的時間。

協力廠商檔案共用也可能所費不貲：當您新增使用者時，您就必須新增授權，而且您可能無法使用現有投資 (如應用程式及內容儲存區)。

協力廠商及自訂應用程式

如果您請協力廠商開發人員為您開發應用程式，就只能仰賴自己的廠商。防止資料外洩 (DLP) 可能未內建至應用程式。

您可以嘗試開發專屬的應用程式，但您需要員工支援開發，而且可能必須因應新裝置類型、作業系統更新所需的任何變更。

許多安全性專家、頂尖聯邦政府網路安全官員，以及國會領導人都要求加強持續監控、自動化監控工具和迅速反應對政府資訊技術系統的攻擊。

原則的重要性

如果您想要讓使用者在個人裝置上存取公司資源，則需要建立原則以規範資料存取和使用的方式。

您可以先要求使用者輸入密碼，然後才能存取重要資料。

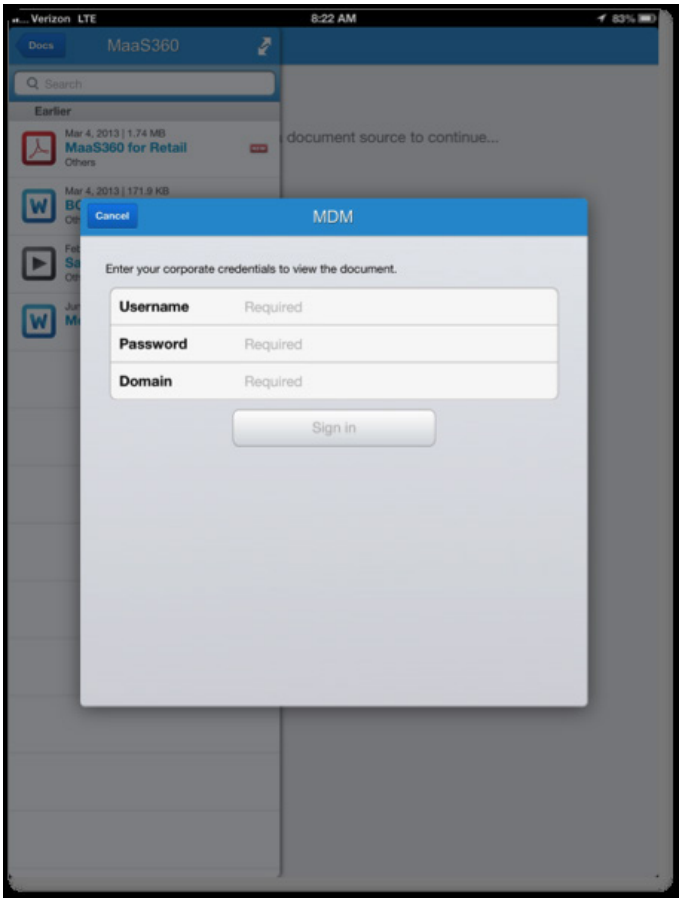

圖 1：驗證要求

您也可以限制剪下和貼上文件中的文字。

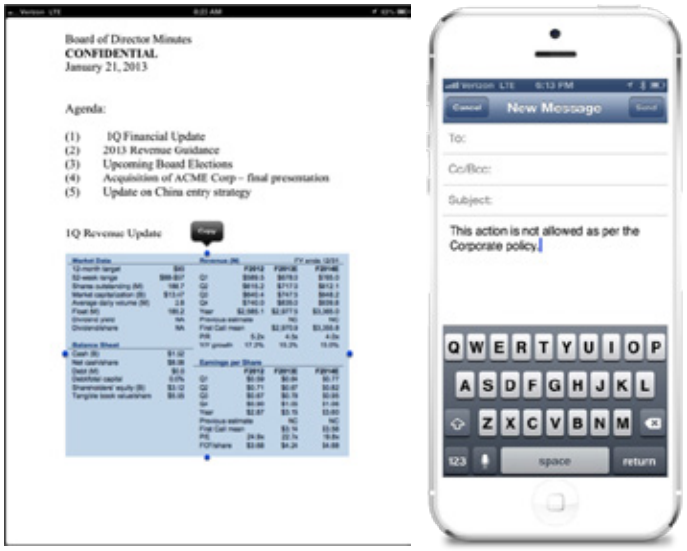

圖 2：防止資料外洩的控制項，例如限制複製和貼上

IBM® MaaS360® 生產力套件

MaaS360 Productivity Suite 可協助您克服最新技術產生的挑戰，並設計為可用多種方法來進行安全存取和保護待用資料：

1. IBM® MaaS360® Secure Mobile Mail
2. IBM® MaaS360® Mobile Application Security
3. IBM® MaaS360® Secure Mobile Browser

MaaS360 使用容器以進行雙重角色方式，也就是公司專屬的資料、應用程式及內容會放在裝置上的受保護區域中。您可以決定要在受保護區域中放置哪些控制項，讓郵件、聯絡人、行事曆、應用程式 (及應用程式資料)、文件和網頁的存取能夠受到保護。

圖 3：MaaS360 Productivity Suite 及 MaaS360 Content Suite

MaaS360 Productivity Suite 使用角色原則，以便在所有使用者裝置上指定安全性。這些原則是在 MaaS360 入口網站中建立並透過無線方式部署至已註冊裝置，如此 IT 就不需要實際接觸裝置。

如果裝置未遵循規定，或是專案已經結束且廠商離開，您只需要遠端移除容器，資料和應用程式便會消失。

容器有內建的安全性，其中包含符合 FIPS 140-2 標準的 AES-256 加密。您可以要求使用者在存取時輸入密碼。如果裝置遭到破解或刷機，或是如果裝置並未在指定的期間內簽入，您也可以使用這些原則設定來完全移除容器。

您也可以防止檔案遭到移動、複製或是從容器列印，而且您可以防止檔案被匯入其中。

IBM® MaaS360® Content Suite

MaaS360 Content Suite 提供加密的容器和生產力工具，以便在行動裝置上散發、檢視、建立、編輯和共用文件，賦予組織所需的控制能力以及員工需要的存取權：

1. IBM® MaaS360® Mobile Content Management
2. IBM® MaaS360® Mobile Document Editor
3. IBM® MaaS360® 行動文件同步

MaaS360 Mobile Content Management 針對內容協同作業提供行動文件容器，其中具有一組穩健強大的生命週期管理功能，以便散發、更新、管理和保護文件。IT 管理員可強制執行驗證、複製/貼上和僅限檢視等限制。使用者可存取公司散發的內容和檔案儲存庫 (例如，SharePoint、Box 及 Google Drive)。

MaaS360 Mobile Document Editor 的設計旨在防止公司資料外洩，同時還能讓使用者建立、編輯和儲存文件。使用者可以在外出時，在行動裝置上協同合作 Word、Excel、PowerPoint 及文字檔案。

MaaS360 Mobile Document Sync 可讓使用者輕鬆地在受管理行動裝置上同步處理內容，以便繼續建立或編輯其檔案，而不會遭到中斷。IT 可以將原則 (例如，限制複製/貼上，以及在未受管理應用程式中封鎖開啟或分享) 套用到內容。這些控制項可以套用到所有文件、文件群組或個別文件，讓您有靈活彈性來保護寶貴的公司資料。

共用受保護內容的使用案例幾乎在所有組織中都是不勝枚舉的，無論是在銷售、行銷、營運或財務部門都是這樣：

- 在外出與客戶開會之前，隨時檢視和共用對銷售簡報進行的最後一刻變更
- 在登機之前，在試算表上合作最新的財務報表

- 在咖啡廳時腦力激盪行銷訊息並與同事分享內容
- 將季度財務文件提供給董事會並將文件到期時間設定為會議之後
- 與銷售團隊分享近乎即時的產品資料，如此他們就不需要手忙腳亂地尋找最新的資料表或競爭資訊
- 確定零售商店中的平板電腦具有最新的產品和庫存資訊

IBM® MaaS360® Gateway Suite

MaaS360 Gateway Suite 是實現這所有一切的關鍵元件。它可以提供完美順暢且受保護的存取權，讓使用者從行動裝置存取您的公司內容和內部網路，以保護傳輸中的資料：

- 提供資料的簡易、受保護行動存取權，而不需要使用裝置上 VPN；您不需要在每次需要資訊時登入 VPN
- 賦予 SharePoint、Windows 檔案共用、內部網站和 Web 應用程式行動能力
- 利用穩健的安全性原則和 DLP 控制項保護資料
- 不需要變更您的網路或防火牆安全性設定

圖 4：MaaS360 Gateway 的資料流程

您可以設定原則選項來管理 MaaS360 Productivity Suite 與使用者裝置互動的方式。例如，您可以指定公司維基百科的 URL、錯誤追蹤系統等，或是透過 MaaS360 Gateway 存取的公司資料夾，而且它們會在 MaaS360 Secure Mobile Browser 中顯示為書籤。您也可以指定是否需要授權才能存取這些位置。

MaaS360 Gateway 會決定當使用者在裝置上存取資料容器時，他們能看到哪些公司資源。

先試用再購買

試用 MaaS360 非常容易且快速，而且您花費在配置 MaaS360 的時間絕對是值得的。如果您認為 MaaS360 是適合組織的解決方案，試用環境就會成為真實環境！

如需 MaaS360 的免費試用，請 按一下此處. 您可以立即開始試用，沒有複雜的設定程序也不需變更基礎架構。立即試用 MaaS360！

圖 5：MaaS360 產品

關於 IBM MaaS360

IBM MaaS360 是企業行動力管理平台，可針對人員工作的方式啟用生產力及資料保護。數萬個組織都相信 MaaS360 能作為其行動力先導計畫的基礎。MaaS360 提供全方位管理以及跨使用者、裝置、應用程式及內容之間的堅實安全性控制力，以支援任何行動部署。如需 IBM MaaS360 的詳細資訊並開始使用免費 30 天試用版，請造訪 www.ibm.com/maas360

關於 IBM Security

IBM 的安全性平台提供安全性智慧，以協助組織全面保護其人員、資料、應用程式及基礎架構。IBM 提供解決方案以用於身分識別及存取管理、安全性資訊和事件管理、資料庫安全性、應用程式開發、風險管理、端點管理、新一代入侵保護及其他。IBM 營運全球最廣泛安全性研究及發展和交付組織之一。如需更多資訊，請造訪 www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美國印製 2016 年 3 月

WGW03111-TWZH-01