IBM MaaS360 行動應用程式管理

只要部署、管理和確保行動應用程式安全無虞

主要優勢

- 利用「容器化」保護企業應用程式
- 提升員工產能及滿意度
- 利用 Web 型主控台，集中管理行動應用程式
- 安全地支援 BYOD
- 降低敏感性資料外洩的風險
- 利用政策及規定，強制執行裝置上存取控制和合規性
- 對應用程式目錄及受管理的應用程式執行選擇性的抹除作業
- 使用精細的管理控制和互動式的圖形化報告
- 降低網路負載和提升應用程式效能及可擴充性

提供應用程式的受保護存取權限

智慧型手機及平板電腦已經藉由提升產能、改善效率及增強客戶滿意度而完全改造企業。但是，若未能確保敏感性企業資料安全無虞，行動裝置數量的暴增現象將無法讓我們高枕無憂，特別是在這個流行自攜設備 (BYOD) 的時代。

這不再只是控制電子郵件和管理裝置。行動應用程式徹底釋放行動裝置的真正潛能。

但是，有鑑於成效不彰的資料儲存作法、惡意程式、未經授權的存取、缺乏加密和因為同步處理而導致資料外洩，因而使得行動應用程式卻逐漸成為企業安全性弱點的來源。

有超過 100 萬個各具特色的行動應用程式，可供您的員工在智慧型手機和平板電腦上安裝和使用。[1]

企業需要在個人或公務裝置上散發、管理及確保業務關鍵型行動應用程式安全無虞的能力。

IBM® MaaS360® 行動應用程式管理可簡化行動應用程式管理，方法是提供直觀式企業應用程式目錄和穩健安全性和應用程式的作業生命週期管理。

「在 2017 年，25% 的企業將會有企業應用程式商店來管理 PC 和行動裝置上獲企業批准認可的應用程式」[2] – Gartner

企業應用程式目錄

- 為 iOS、Android 及 Windows Phone 裝置提供直觀式、可自訂企業應用程式目錄
- 提供卓越的使用者經驗
- 即時協助使用者檢視可用的應用程式、安裝應用程式和獲得警示以更新應用程式
- 散發精選的公用和企業應用程式
- 使用受保護、Web 型主控台以管理和散發應用程式

*圖 1：*行動裝置上企業應用程式目錄的範例

行動應用程式生命週期管理

- 使用最佳作法行動應用程式管理工作流程
- 散發應用程式及追蹤其無線 (OTA) 安裝至所有使用者、使用者群組或個別裝置
- 發佈應用程式更新
- 參照持續應用程式庫存報告
- 與 Apple App Store、Google Play 及 Windows Phone Store 等公開應用程式商店整合，以打造順暢完美的工作流程。

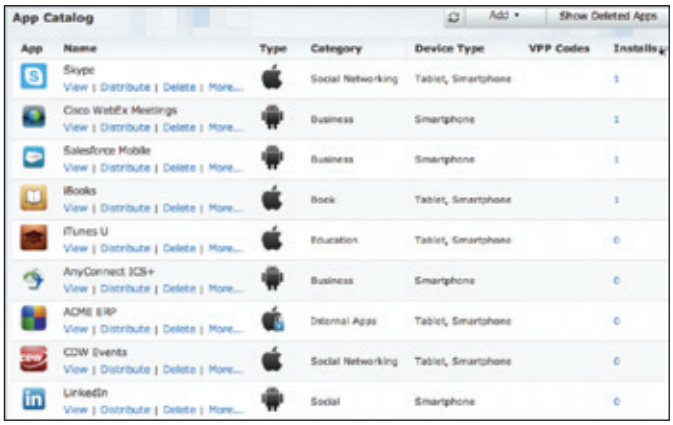

*圖 2：*MaaS360 入口網站中應用程式目錄的範例

IBM® MaaS360® 行動應用程式安全性

- 將簡單的應用程式包裝函式或軟體開發套件 (SDK) 作為 MaaS360 行動應用程式管理的安全性附加程式
- 先驗證使用者，然後再存取應用程式
- 強制執行裝置合規性檢查
- 限制複製和貼上，以及本機和雲端資料備份
- 收到關於合規性違規的近乎即時警示
- 應用程式等級通道服務，能以受保護的存取權限使用企業資料，而不需要裝置 VPN

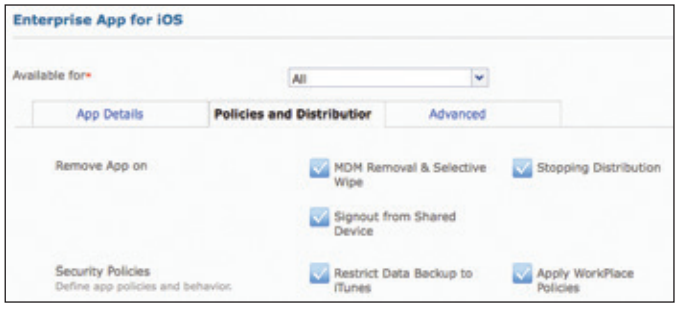

*圖 3：*可針對應用程式設定之安全性選項範例

行動應用程式合規性及實施

- 黑名單、白名單和設定必要應用程式
- 限制裝置上的原生應用程式 (例如，YouTube)
- 限制越獄裝置狀態或根目錄權限裝置的存取權限
- 設定自動化合規性實施動作
- 透過自動化或手動介入以封鎖電子郵件存取、限制網路資源 (例如，無 VPN) 和執行遠端抹除，以採取即時動作
- 檢視安全性及合規性歷史的圖形化報告

*圖 4：*顯示如何將應用程式設定為黑名單，以便無法將之安裝在裝置上的範例

企業行動應用程式容器

MaaS360 行動應用程式管理會簡化應用程式管理，方法是提供易於使用使用企業應用程式目錄和穩健安全性和應用程式的作業生命週期管理。

企業應用程式目錄

適用於 iOS、Android 及 Windows Phone 的直觀式、可自訂企業應用程式目錄。

行動應用程式生命週期管理

可散發、更新、管理及保護公開及企業行動應用程式的平台。

行動應用程式安全性

企業應用程式的行動應用程式容器，具備可作為 MobileFirst Protect 應用程式之MaaS360 行動應用程式管理。

行動應用程式合規性及實施

適用於黑名單、白名單及必要應用程式的安全性政策。自動化實施規定以警示管理員、封鎖電子郵件、限制網路資源和執行遠端抹除。

IBM® MaaS360® 內容服務

在全球最佳化應用程式散發網路上託管和散發企業行動應用程式的選項。

大量購買方案

支援適用於員工的大量應用程式授權。

若要瞭解有關 IBM Security 預防詐騙解決方案的更多資訊，請與您的 IBM 業務代表或 IBM 事業夥伴聯絡，或造訪以下網站：**ibm.com**/security.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美國印製 2016 年 1 月

本文件內容為截至初始發佈日期時的最新資訊，且得由 IBM 隨時進行變更。並非在 IBM 營運的每個國家/地區均提供所有產品。

所載之效能資料及客戶範例展示僅作圖解用途。實際的效能結果會依據特定配置及操作條件而有所不同。使用者有責任評估並確認任何含有 IBM 產品及程式的其他產品或程式，在運作上是否正常。

本文件中的資訊係以「原樣」的原則提供，且不包含任何明示或暗示的保證，包括對適銷性、針對特定用途適用性的任何保證，以及不侵權的任何保證或條件。IBM 產品根據提供這些產品時所依據的協定的條款與條件進行保證。

客戶有責任確認自己是否遵循適用法律及法規。IBM 不提供法律建議，亦不聲明或保證其服務或產品將確保客戶遵守任何法律或規定。

關於 IBM 未來方針或目的之聲明僅代表其目標與目的，可能隨時變更或撤銷，恕不另行通知。

良好安全性實務的聲明：IT 系統安全性涉及透過保護、偵測和回應企業內部和外部的不當存取來保護系統及資訊。不當存取可能導致資訊遭到變更、銷毀或挪用，或是造成毀損或濫用您的系統（包含攻擊其他人）。不應該將任何 IT 系統或產品視為完全安全無虞，而且沒有任何單一產品或安全措施對於保護不當存取完全有效。IBM 系統及產品設計旨在成為全面性安全性方法的一部分，其中會一定涉及其他作業程序，而且可能會要求其他系統、產品或服務要達到最有效的狀態。IBM 不保證系統及產品可免於任一方的惡意或非法行動的攻擊。

請回收

1 截至 2014 年 7 月，在領先業界的應用程式商店中可用的應用程式數量，Statista， http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

2 「*Gartner 表示到 2017 年，25% 的企業都會有企業應用程式商店，*」Gartner Group 新聞稿，2013 年 2 月 12 日，http://www.gartner.com/newsroom/id/2334015

WGD03060-TWZH-01