IBM Security
創新思維領導白皮書

行動應用程式生命週期管理的最佳作法

從設計到部署的安全性

IBM

安全性在行動應用程式開發所扮演的角色

行動裝置現在已經在許多組織中廣泛運用。採用行動裝置管理 (MDM) 及行動應用程式管理 (MAM)，組織逐漸針對特定工作開發企業專屬的應用程式，以提升生產力、事業合作夥伴關係、客戶滿意度和利潤表現。然而，為了達到這些利益，重要的是必須在整個應用程式生命週期期間納入行動安全性最佳作法。

組織面臨全新挑戰：如何將合規性及安全性最佳作法延伸至筆記型電腦及其他行動裝置。

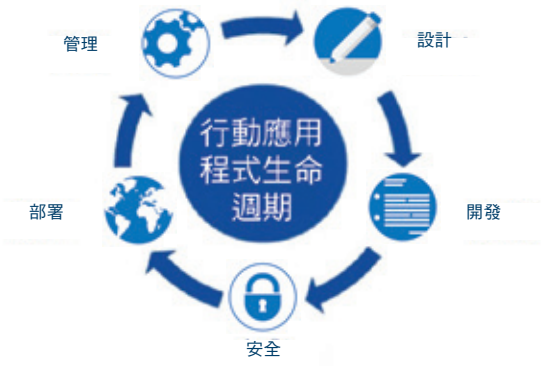

圖 1：行動應用程式生命週期包含建立、保護和管理應用程式

行動應用程式生命週期管理 (MALM) 承接了自行動世代以來便已存在的所有問題 - 安全性、合規性和隱私權。這包含公司和個人資料的安全性、遵循政府和產業法規，以及員工隱私權。建立自訂行動應用程式的過程可能看似繁瑣，但更大的挑戰在於部署之後，要如何保護應用程式和相關聯的資料。

IBM Security 是企業行動力管理 (EMM) 領域備受認可的領導者，提供應用程式安全性最佳作法，以便在應用程式開發和部署期間使用。對於設計及開發其專屬行動應用程式的企業而言，這些功能可透過軟體開發套件 (SDK) 或自動應用程式封裝加以提供。

主動式應用程式安全性最佳作法

當應用程式可供部署時，設定安全性原則並加以實作是很好的做法，但是將安全性整合至應用程式的設計和開發中，卻可以隨時間簡化和強化您的工作。除了可隨裝置作業系統提供的資料加密以外，還有數個可透過 MaaS360® 而在應用程式開發期間新增的主動安全性功能。這些功能包括：

驗證

除了具備 MaaS360 (其可包含基本密碼註冊，或是利用 Active Directory 或 LDAP 同步之雙重因素驗證) 的裝置驗證以外，您還可以將驗證內嵌到應用程式中。只有預定要存取特定應用程式及相關聯資料的使用者可以開啟這些程式，即使是誤將應用程式散發給未經授權的使用者亦然。

單一登入

您可以將應用程式設計為使用者只需以單一、共用的密碼就能存取他們獲得授權的所有企業應用程式。在使用開發人員平台 (例如 IBM Worklight) 建立行動應用程式時，MaaS360 的這項支援特性就會提供更加以使用者為中心的處理方式。® 您可以

協助確保堅實驗證，而不會影響使用者的生產力。IBM® MaaS360® Trusted Workplace 可簡化跨行動平台的應用程式設計，讓驗證、單一登入、資料外洩防護 (DLP)、應用程式內 VPN 和應用程式封鎖的設計變得容易。

資料外洩防護 (DLP)

MaaS360 支援雙重角色環境，其會區隔行動裝置上的公司和個人資料。開發人員及 MDM 管理員能以各種方法使用這個受保護的容器 (MaaS360 Trusted Workplace)，來防止資料外洩、阻止公司和個人資料混合，以及解決任何員工隱私權問題。

- **MaaS360 Trusted Workplace：** 此容器具備符合 FIPS 140-2 標準的 AES-256 加密功能，可受密碼保護，而且未經裝置擁有者驗證是無法存取的。若裝置遺失或遭竊，公司應用程式、文件及資料會保持受保護狀態，而且會回報事件並遠端抹除容器。即使員工因為遺失裝置不好意思而延誤幾天通知 IT，公司資訊還是會受到保護。
- **選擇性抹除：** 幾乎所有透過 MaaS360 推播至裝置的資訊都能在遠端從容器抹除，而不會影響使用者基於個人用途而下載的資訊 (MaaS360 也提供完整抹除功能，可將裝置還原為原廠設定)。
- **限制複製和貼上：** MaaS360 可提供禁止在容器外部複製和貼上資訊的功能。如果使用者嘗試將容器中的資料貼到可從其個人空間存取的資源 (例如，記事本、原生電子郵件應用程式、檔案共用網站或備份資料雲端)，則會改為貼上提醒訊息，向使用者提醒您公司的安全性政策。同時也會自動將關於嘗試進行該活動的警示傳送給 MaaS360 管理員。
- **開啟於控制項**: MaaS360 也提供「開啟於」控制項，讓使用者只能在 MaaS360 Trusted Workplace 容器中使用屬於公司和受公司控制的應用程式來開啟文件和檔案。無法在容器外部開啟或移動公司資訊。

因為管理階層及 IT 人員無法直接控制行動裝置，所以特別容易因為員工所犯錯誤和不正確的行為而產生漏洞。

應用程式內 VPN

雖然上述所有功能都能強化待用資料在行動裝置上的安全性，但企業應用程式開發人員也必須保護傳輸中的資料，例如，任何從 MaaS360 Trusted Workplace 容器傳輸到公司伺服器的資訊。為了保護那些傳輸內容，必須要提供 VPN 連線。應用程式層級的通道可協助確保：只透過應用程式層級的 VPN 連線就能安全地傳送使用者所傳輸的資料，而不需要裝置層級的 VPN。借助 IBM® MaaS360® Gateway for Apps，不需要使用任何 VPN 基礎架構就可以達到這個目的。

應用程式封鎖

您的應用程式開發也可以設定原則來封鎖應用程式，使其無法在與 MaaS360 自動安全性監控功能不相容的裝置上開啟。

企業應用程式商店最佳作法

開發應用程式之後，簡單而安全的散發及控制方法就是使用企業應用程式商店。事實上，許多 MaaS360 客戶已經使用系統的 App Catalog 功能來管理來自於 iTunes App Store、Google Play 及 Windows 市集等商店的公用應用程式以及企業內部應用程式。藉由搭配使用 MaaS360 Trusted Workplace 容器和 MaaS360 App Catalog，還可以更精細地控制應用程式。透過此方法，IT 所取得的應用程式 (無論是協力廠商製作或自行研發) 都能完整與個人應用程式區隔開來。

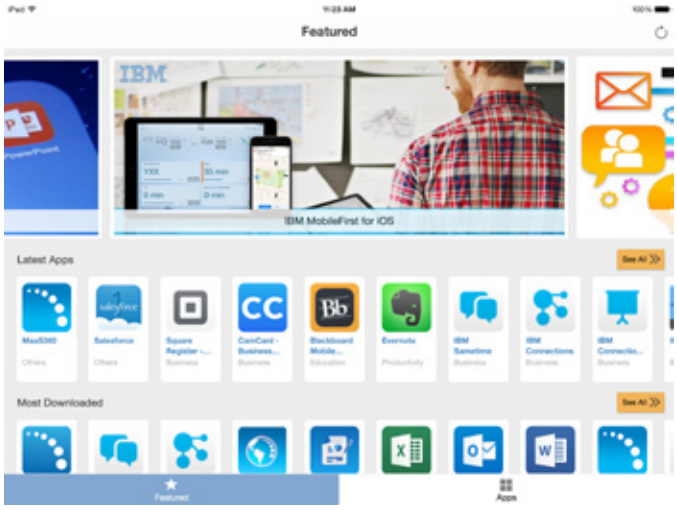

圖 2：應用程式目錄可讓使用者輕鬆找到核准的應用程式

完全整合應用程式商店的優勢

MaaS360 App Catalog 提供與行動作業系統無關的整合介面，如此您就能從一個視窗跨多個平台來管理應用程式。完全整合的應用程式商店的其他優勢：

部署及更新應用程式，而不會有所延遲

除了您自訂的企業應用程式以外，App Catalog 還能與公用應用程式商店整合。您可以利用大量散發功能將 應用程式推播到個別裝置、使用者群組或所有使用者，並即時追蹤其安裝情況。例如，如果您希望使用 Apple 大量購買方案 (VPP)，將購買的 iOS 應用程式提供給員工，則可透過 MaaS360 直接上傳 VPP 檔案和管理那些授權。如果使用者離職，您可以從其裝置移除該應用程式並重新分配授權。如果使用者必須刪除應用程式然後再重新安裝，則無需聯絡 IT 以取得另一個授權，也無需透過公用應用程式商店取得。相反地，他們只需要前往組織的 App Catalog 並點擊應用程式的「安裝」按鈕即可。

與現有的企業安全性及身份識別基礎架構整合

許多組織都需要為特定使用者群組部署應用程式。雖然您可以在 MaaS360 中設定使用者群組，但為了協助確保將適當的應用程式散發給適當的人員，若利用現有架構在 Active Directory 或 LDAP 上的使用者身份識別來配合企業行動力，則可以省下不少心力。您可以利用 MaaS360 Cloud Extender 達成這個目的。對於自訂功能，我們強烈建議使用 Web 服務將 MaaS360 與不同類型的 IT 基礎架構整合在一起，因為它們穩健強大、有彈性、有效率、易於撰寫程式碼，而且容易發佈到網際網路，同時還能讓應用程式、文件及資料保持受保護的狀態。

穩健控制應用程式安全性及管理

透過 MaaS360 進行管理時，自訂企業應用程式能與其他應用程式獲得相同程度的保護 (請參閱下一節，以瞭解 「被動式」應用程式安全性最佳作法)

應用程式版本控制

若使用公用應用程式，您通常只能為所有預定使用者提供應用程式的某一個版本。若使用自訂的企業應用程式，無論是由內部或是由協力廠商開發而成，您可能會有該應用程式的更新版本，而您希望先推播給少數幾個人，之後再向整個企業發佈。使用 MaaS360，您就能部署和管理相同應用程式的不同版本。

應用程式探索和使用者協同作業

使用者必須能夠探索和存取組織建議或要求用於執行作業的授權應用程式。有了 MaaS360 中的應用程式探索入口網站，就能在易於使用的介面中輕鬆找到應用程式。使用者也可以安全地分享和連結那些核准用於 Trusted Workplace 容器的應用程式。他們可以對應用程式發表意見和評分以協助識別其實用性，並輕鬆與人溝通哪些應用程式需要更新或增強以提升工作價值。

隨需應用程式庫存控制及報告

您的 MaaS360 管理員可以依需要查看和回報 App Catalog 中所有可用的應用程式、獲授權的使用者，以及每個使用者裝置上的 WorkPlace 容器中的應用程式。管理員可以刪除任何使用者、群組或所有裝置的應用程式 (例如，已更新應用程式的舊版)。

更精密的產品也逐漸面世，可以監控和記錄將機密檔案傳輸到儲存裝置以及透過電子郵件、檔案傳輸或即時傳訊等方式傳輸到其他電腦的傳輸作業，也可以完全封鎖所有此類傳輸。

只考慮一個平台，以獲得簡易操作性和安全性

有了 IBM Worklight，只需要使用一個視窗，就能進行跨行動平台的應用程式開發。有了 MaaS360，透過一個視窗即可進行跨平台的 MDM、MAM 及 MALM。這些整合式方法可藉由提高控制力、安全性、合規性及生產力，來增加企業行動力的優勢，同時還能降低對於資源、時間和預算的需求。

「被動式」應用程式安全性最佳作法

透過 MaaS360 進行管理時，公用及企業應用程式具有相同的組織控制和保護，例如：

- 應用程式白名單設計和黑名單設計
- 設定安全性及限制
- 自動對未合規裝置強制執行某些動作 (警示、封鎖裝置、選擇性或完全抹除裝置)
- 自動監控越獄、植入根目錄和不符合規定的裝置
- 可持續看見裝置的合規性狀態
- 報告安全性及合規性歷史

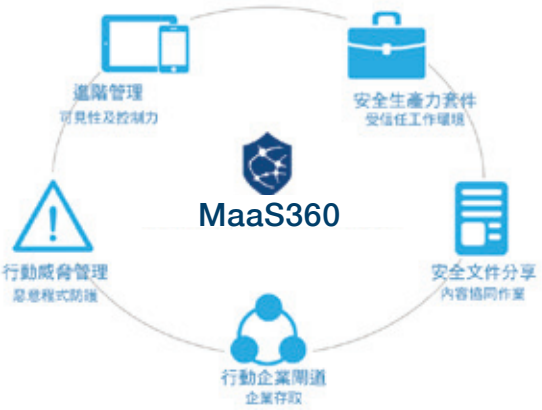

圖 3：MaaS360 的五大關鍵重點

IBM® MaaS360® Secure Mobile 瀏覽器

許多組織都已經挹注大量資源，而且擁有仰賴現有 Web 應用程式的完善商業程序。有了 MaaS360 Secure Mobile Browser 及 IBM® MaaS360® Gateway Suite，您就能讓員工在受保護的情況下，從行動裝置存取公司內部網路網站及應用程式 (如私人 SharePoint、Windows File Sharing 和內部網站)。這可讓您行動化所有網頁，而不需要將之重新撰寫為行動應用程式或是設定完整的裝置層級 VPN。

MaaS360 Secure Mobile Browser 也能讓您的 MaaS360 管理員依類別限制從任何裝置存取網站的權限，以及制訂因為商業目的而存取限制內容的例外情況。例如，如果您的組織將社群網站設定為黑名單，管理員就可以基於商業目的視需要為行銷或公關人員制定例外情況，使其能夠使用 LinkedIn。如果其他人嘗試存取社群網路，則會拒絕存取 (管理員會取得包含時間和日期戳記的稽核記錄檔，以識別嘗試存取限制網站之每一個實例中的使用者和裝置。您可以透過 MaaS360 傳訊系統警告重複違規者)。

IBM® MaaS360® 行動應用程式安全性 SDK

MaaS360 行動應用程式安全性 SDK 可讓開發人員將 MaaS360 穩健強大的安全性功能內嵌到其應用程式中，做為可設定的安全性層，而且只需幾小時就能完成。SDK 可讓開發人員將穩健強大的安全性功能內嵌到其應用程式中，做為可設定的安全性層，而且只需幾小時就能完成。另一個選項是在彈指間，利用應用程式封裝內嵌這些安全性功能。企業應用程式可依據應用程式確切的需求來調整所有 MaaS360 防護功能，方法是在開發期間整合 SDK。SDK 也可讓開發人員整合 MaaS360 及 iOS、Android 和 Windows Phone 裝置中內建的許多功能。

MaaS360 即時應用程式封裝

對於已經開發完成的應用程式，MaaS360 應用程式封裝會自動將必要程式碼嵌入您的應用程式中。您只需要點擊按鈕，就能在彈指間加入 MaaS360 穩健強大的應用程式安全性及管理功能。

另一個邁向企業行動力的關鍵步驟

BYOD 花了好幾年時間才讓組織接受這個概念，不過 MALM 應該能較快實現。企業行動力的價值會隨組織的任務和作業方式而調整，這在生產力、客戶及合作夥伴關係、員工滿意度和利潤表現等方面都是不可否認的。從聘僱到離職面談，員工的行動電話最終都是組織內部授權的數位和實體資產的主要存取點。如果行動安全性可以為資訊提供和固定 IT 基礎架構相同程度的保護，自訂企業行動應用程式就會是許多組織亟欲採取的關鍵後續步驟。MaaS360 已經協助全球上千個組織確保其行動先導計畫能利用解決方案來解決 MDM、MAM 及 MALM 的問題，而且此類解決方案能讓 IT 快速實作和管理、能輕鬆讓使用者接受，而且迅速靈活能因應瞬息萬變的行動世界。

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

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

WGW03110-TWZH-01