IBM Security
創新思維領導白皮書

行動裝置是竊賊的新遊樂場

如何防範行動惡意程式

IBM

隨著行動裝置的成長，威脅也相對增加

簡介

行動力以前所未有的速度促進企業轉型，伴隨持續大量增加的智慧型手機，爆量開發的行動應用程式，以及對工作檔案的存取增加。組織採納自攜裝置 (BYOD) 的政策，甚至允許將個人應用程式用於處理工作相關活動，讓員工幾乎能夠隨時隨地提升生產力。

但是，組織並未透過部署保護其敏感性資訊所需的企業級安全性，而跟上這項行動力爆炸的步調。駭客和竊賊都把握這個機會，透過行動端點滲透網路並取得敏感性工作資料。IT 及安全性主管需要現代化且穩健的安全性解決方案，以主動偵測，分析和補救這些行動威脅。

在任何時間，大約都有 1,600 萬個行動裝置會受到惡意程式感染。

企業的行動裝置爆量

與行動力成長相關聯的數字成長驚人。預測行動電話數量 (73 億) 在 2014 年將超過地球總人口數量 (70 億)。[1]

根據 Arxan Technologies 的報告，2014 年總共下載了 1,380 億個行動應用程式，而且此數字預期在 2017 年將會翻倍成長，而達到 2,680 億。[2]

消費者因為採用智慧型裝置和應用程式以用於個人用途，而成為這項行動運動的初始催化劑；然而，企業當然也從這些加速趨勢獲益不少。工作場所的 BYOD 趨勢持續擴散，可協助組織行動化其整個工作團隊，而可節省採購和支援成本。事實上，Gartner 預測在 2017 年有超過半數的員工會需要 BYOD。[3]

行動應用程式正在為員工建立全新且有效率的工作流程。順暢存取工作資料，電子郵件和內容的需求也在增加，因此提升了產能收益。組織開始針對每個程序思考「行動優先」，進一步實現企業中的行動力成長情況。

遭到行動應用程式攻擊時

但是，駭客和竊賊威脅要竊取企業轉型所帶來的這些龐大利益。行動裝置遭到感染的數量在 2014 年加速增加 25% (與 2013 年的 20% 相比較)，並且在任何時間，預估大約都有 1,600 萬個行動裝置受到惡意程式感染。[4]

行動惡意程式是特別建立來攻擊行動裝置的惡意軟體，它是利用特定作業系統的漏洞來進行。

資料漏洞的影響可能所費不貲，而這對於公司品牌形象的傷害則會因為潛在的財物損失而加劇。Ponemon Institute 在 2014 年預估單一漏洞的成本是 350 萬美元，比一年前增加了 15%。[5]

圖 1：熱門的付費 Android 及 iOS 應用程式已遭到駭客入侵

通常，因為惡意行動應用程式而遭到危害的裝置幾乎是所有企業的最大風險來源。根據 Arxan Technologies 調查，當使用者連結不安全的網路或是從不安全的來源安裝具風險的應用程式時，行動裝置很容易遭到惡意程式攻擊。分別有 97% 及 87% 的熱門付費 Android 及 iOS 應用程式已遭到駭客入侵，並張貼到協力廠商應用程式商店中。[6]

如同在另一份 Ponemon Institute 研究中所揭露[7]，即使應用程式來自於受信任的組織並且是透過傳統應用程式商店取得，也可能帶來巨大風險。82% 的受訪者表示工作環境中的行動應用程式已經大幅度 (50%) 或是顯著 (32 %) 增加了安全性風險。雖然大多數的員工都是「應用程式的重度使用者」(66%)，超過一半 (55%) 的受訪者表示其組織並未制定定義工作場所中可使用行動應用程式的政策。

只有 30% 的受訪者表示其組織已部署企業應用程式商店，雖然大部分 (67%) 的受訪者承認即使他們有應用程式商店，員工還是可能使用來自其他來源的未審核行動應用程式。此外，有 55% 組織表示他們允許員工在其個人裝置上從企業應用程式商店下載和使用工作應用程式。

最新狀態的行動惡意程式

什麼是行動惡意程式？

行動惡意程式是特別建立來攻擊行動裝置的惡意軟體，它是利用特定作業系統的漏洞來進行。三種常見惡意程式類型是：

- 間碟軟體 - 裝置資料竊賊和間碟會擷取特定種類的資料，然後將之提供給駭客以獲取利益
- 特洛伊木馬病毒 - 這種惡意程式會影響裝置或應用程式的功能，進行自動化交易，或是在使用者不知情的情況下初始化通訊
- 破解或刷機惡意程式 - 賦予駭客特定的裝置管理權限及檔案存取權

若要瞭解威脅及其著重於行動端點的原因，讓我們來看看網路犯罪者精心思考的程序。行動裝置是取得敏感資料最簡易的路徑之一。企業後端系統受到防火牆，入侵預防系統及防毒閘道的完善保護時，公司或個人裝置通常不會採用相同等級的保護。個人裝置 (BYOD) 特別脆弱，因為它們不屬於周邊設備且通常不在組織控制範圍內。

如果駭客能夠攻擊端點，則可使用惡意程式以便對使用者進行社交工程，從而擷取個人可識別資訊 (PII) 與憑証。他們可以接手使用者的帳戶並善用驗證的工作階段，以蒐集私人資料和執行詐騙交易。

Android 數量過多的憂慮

根據 IDC，Android 掌控行動裝置市場並擁有 81.2% 的市占率，而且在 2014 年的裝置出貨量超過 10 億。[8] Android 目前掌控消費者市場，但企業的採用速度仍然極為緩慢。

基本設計及平台開放性和應用程式生態系統，這些都是 Android 為何會成為今日行動產業中最容易遭受惡意程式感染的其中一個系統的原因。

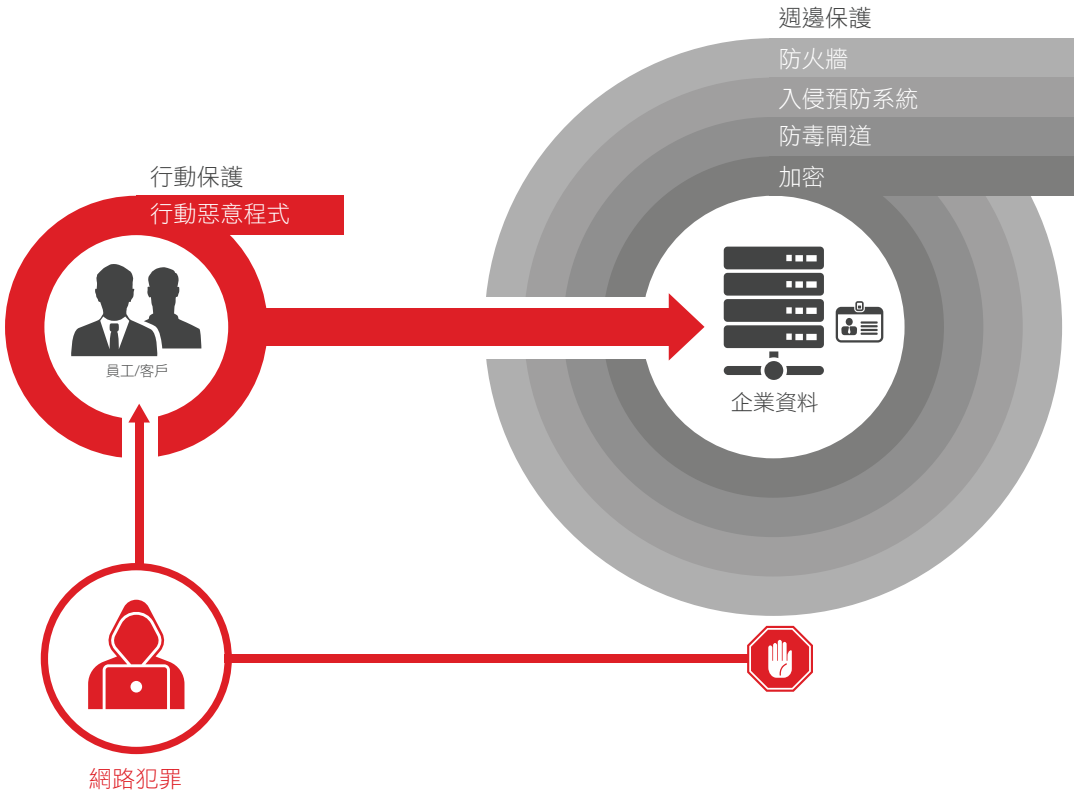

圖 2：犯罪者會攻擊最脆弱的連結以存取敏感性資料

基本設計及平台開放性和應用程式生態系統，這些是 Android 為何會成為今日行動產業中最容易遭受惡意程式感染系統之一的原因。下列特性使得 Android 成為駭客及竊賊最容易下手的目標之一：

- 可透過協力廠商應用程式商店和網站下載和安裝 Android 應用程式。
- Google Play 商店並不會像 Apple 那樣密集地審核和核准每個應用程式，Apple 會先這麼做，然後才將 iOS 應用程式發佈到 iTunes。
- 簽署 Android 應用程式的數位憑證未受到控制。這些應用程式通常是自我簽署且無法追溯至應用程式開發人員。這使得駭入 Android 應用程式， 注入惡意程式並重新簽署變得輕而易舉。

網路犯罪者持續探索全新和創意的方式來攻擊不同於 PC 之行動作業系統平台上的弱點。

Google 已經實作安全性作法以清除 Google Play 商店中的惡意應用程式。它會在上傳至商店時掃描應用程式，執行每個應用程式以偵測和移除惡意程式，間諜軟體和特洛伊木馬病毒。當 Google 偵測到新的惡意程式時，其系統可透過所有 Google Play 恢復並從商店移除可疑的檔案。如果違反公司的條款和內容政策，Google 也會停用開發人員應用程式和帳戶。

但是，如前所述，97% 的熱門付費 Android 應用程式已經遭到駭客入侵，而且可在協力廠商的應用程式商店或網站上找到。因此，如果您的員工或其子女在公司或個人 Android 裝置上，從其中一個這種非正式來源免費下載和安裝最新進階遊戲應用程式，您可以預期裝置會受到惡意程式的感染。您的組織可以制定政策和使用者教育訓練，以協助防止這些作法，但如果沒有一層自動化保護，Android 裝置會很容易遭到攻擊。

Android 惡意程式的範例是名為 SVPENG 的銀行特洛伊木馬病毒，它是以俄羅斯和歐洲金融機構為攻擊目標。SVPENG 代表行動惡意程式的重大進展。此攻擊會直接鎖定行動銀行應用程式使用者，方法是使用常見的 PC 惡意程式技術 (名為重疊攻擊) 誘騙受害者提供其認證。

在這個攻擊中，受感染裝置的惡意程式會等候使用者開啟銀行的行動應用程式。惡意程式發現行動銀行應用程式工作階段啟動之後，便會在應用程式上方顯示一個畫面 (亦即「重疊」一詞的由來)，該畫面會模仿銀行應用程式的外觀及操作，但實際上是假造的頁面。這會讓使用者在不知情的情況下與惡意程式產生的頁面互動，他們會認為這是真正的銀行頁面，然後提供銀行認證。

類似的重疊攻擊可能威脅敏感性公司資料。員工可能在不知情的情況下輸入其工作認證，讓竊賊取得所需內容而驗證進入企業系統並肆虐處理您的資料。

最近，IBM X-Force® 應用程式安全研究小組 (Application Security Research Team) 發現 Dropbox SDK for Android 有一個弱點，可讓攻擊者將行動裝置上的應用程式連線至攻擊者所控制的 Dropbox 帳戶，而受害者全程都不知情或未授權。[9] 這項弱點名為 DroppedIn，可透過兩種方式加以利用：使用安裝在使用者裝置上的惡意應用程式，或是從網站遠端使用驅動技術。

這是使用 Dropbox SDK 1.5.4 至 1.6.1 版本之 Android 應用程式內部驗證機制的嚴重瑕疵。IBM Security 小組發現 Dropbox 的問題之後，只花了 4 天，Dropbox SDK for Android v1.6.2 便已解決此問題。DroppedIn 入侵程式的概述位於 SecurityIntelligence.com 上的部落格貼文 (參考註腳 9)。

駭客過去可使用 DroppedIn 入侵程式，因為能輕鬆在 Android 裝置上安裝惡意應用程式。網路犯罪者持續探索全新和創意的方式來攻擊不同於 PC 之行動作業系統平台上的弱點。

雖然 Android 可能持續面臨企業採用的許多挑戰，Google 及裝置製造商的最新安全性進展和領先業界的企業行動力管理 (EMM) 解決方案提供者的支援都有助於在企業和政府機關中擴展版圖。消費者及您的員工選擇使用 Android 裝置時，您的組織需要啟用所需的安全性及保護，才能防範行動惡意程式。

iOS 並非牢不可破

基於數個重要原因，iOS 裝置已經掌控企業市場。當 iPhone 在 2007 年首次面世時，專業人員開始使用其個人 iPhone 處理公務，而不使用公司配給的舊型智慧型手機。除非使用者蓄意繞過其安全性系統，否則基於平台固有設計，iOS 應用程式的沙箱化架構和行為已經能提供安全性，因此駭客難以感染整個裝置和跨應用程式攻擊。

一開始只著重於消費者市場之後，Apple 快速意識到企業市場的潛能。它開始整合控制項，讓 IT 主管借助行動裝置管理 (MDM) 解決方案提供者的協助，更妥善地保護及管理裝置，應用程式和資料。

與 Android 的開放式應用程式架構和生態系統不同之處在於，Apple 傾向於打造比較封閉的裝置和應用程式環境。除非 iOS 裝置遭到破解，否則只能從 iTunes App Store 下載和安裝公用 iOS 應用程式。上傳到 iTunes 的應用程式會經過密集審核程序，然後才會由 Apple 正式發佈。此外，需要數位憑證才能簽署 iOS 應用程式，因此可追溯至應用程式開發人員。

上述所有原因已經使得 iPhone 和 iPad 長久以來深受企業，政府及教育機構歡迎和接受。但是，這些豐富的安全性措施無法阻止網路犯罪者嘗試駭入 iOS 裝置。事實上，駭客會以創意方式感染 iPhone 及 iPad (包含名為 WireLurker 及 Masque Attack 的新惡意程式)。

WireLurker 是同時鎖定 Mac OS 和 iOS 裝置的新種類惡意程式。[10] WireLurker 的獨特之處在於它可以感染未遭到破解的 iOS 裝置，當 iOS 裝置透過 USB 傳輸線連接到受感染的 Mac OS 裝置時就會被感染。

以下是 WireLurker 攻擊裝置的一般方式：

- 使用者在其 Mac OS 裝置上下載並安裝被惡意程式感染的 OS X 應用程式，很有可能是來自於非正式的協力廠商應用程式商店。
- 使用者之後會執行受感染的應用程式並授予其 root 權限，這需要知道 Mac OS 裝置上的管理員密碼。
- 執行時，受到惡意程式感染的 OS X 應用程式會下載數個 iOS 應用程式，然後等候信任該電腦的 iOS 裝置透過 USB 傳輸線連接該電腦。
- 信任受感染 Mac OS 裝置的 iOS 裝置連接之後，惡意應用程式就會將惡意 iOS 應用程式載入到 iPhone 或 iPad 上。
- iOS 應用程式本身是企業簽署的應用程式，這代表網路犯罪者已經危害另一個組織的帳戶，或是讓 Apple 核准其擁有的 iOS 應用程式。這些應用程式也隨附佈建設定檔，如此就會受到 iOS 裝置的信任。

等惡意的 iOS 應用程式上傳到沒有任何懷疑的使用者的未破解 iOS 裝置之後，這些應用程式就可以竊取資訊並定期與攻擊者的伺服器通訊。

最近發現甚至比 WireLurker 更邪惡的惡意程式名為 Masque Attack，[11] 它也可以感染未遭到破解的 iOS 裝置，但並不需要連接到受感染的 Mac OS 裝置。受到這項攻擊時，隨企業/臨機操作佈建的 iOS 應用程式可能會取代 iTunes 應用程式商店所核准的應用程式，只要這兩個應用程式使用相同的組合識別碼即可。

以下是 Masque Attack 能夠取代使用者真正的應用程式並竊取資訊的方式：

- 使用者按一下來自任何網站的連結以下載並安裝使用企業憑證簽署的惡意應用程式 (而且可能會被標示為類似「新版憤怒鳥」這樣的名稱)。
- 惡意應用程式會取代具有相同組合識別碼的合法應用程式 (例如，銀行或電子郵件應用程式)。
- 攻擊者會模仿原始應用程式的登入介面，以竊取使用者的認證。
- 該應用程式也會使用本機資料快取，以模仿所取代應用程式的功能 (例如，電子郵件應用程式的最新電子郵件)。

網路犯罪者持有登入認證和本機快取的資料之後，使用者的機密性資料和財務資訊會容易遭到攻擊和資料遺失。

惡意程式防護符合企業行動力管理

IBM® MaaS360® 行動威脅管理

IBM 藉由整合 IBM Security Trusteer® 為 EMM 提供全新等級的安全性，以防範行動惡意程式和遭到危害的裝置 (例如，遭到破解或刷機的智慧型手機和平板電腦)。

這項獨特整合和協同作業可創造強大的防禦效果，以阻止駭客和竊賊取得公司和個人資訊而獲得犯罪利益。

利用持續更新資料庫中的惡意程式病毒碼來偵測及分析 iOS 和 Android 應用程式。

數百萬個使用者用於保護組織免於遭到詐騙和資料漏洞的 Trusteer，可向 MaaS360 提供風險感知和安全性智慧。

行動惡意程式偵測及修復：

- 利用持續更新資料庫中的惡意程式病毒碼來偵測及分析 iOS 和 Android 應用程式
- 新增應用程式例外情形，以自訂可接受的應用程式使用率
- 設定精細原則控制項，以採取適當行動
- 使用近乎即時的合規性規則引擎以自動緩解
- 偵測到惡意程式時，向使用者和負責任的對象發出警示
- 在「我的警示中心」內檢視遭到破壞的裝置並在「我的活動動態訊息」儀表板中檢視偵測事件
- 自動解除安裝含有惡意程式碼的應用程式 (適用於特定 Android 裝置，如 Samsung SAFE)
- 封鎖存取權限，選擇性或完全抹除裝置
- 收集及檢視裝置威脅屬性，包含：
  - 偵測到惡意程式
  - 找到可疑的系統配置，例如未知的 SMS 接聽程式或啟動套件
  - 連線至不安全的 Wi-Fi 熱點
  - 允許安裝市面上沒有的應用程式
  - 作業系統版本
- 檢閱惡意程式偵測事件的稽核歷史

圖 3：MaaS360 和 Trusteer 搭配使用以偵測，分析行動惡意程式及補救遭到攻擊的裝置

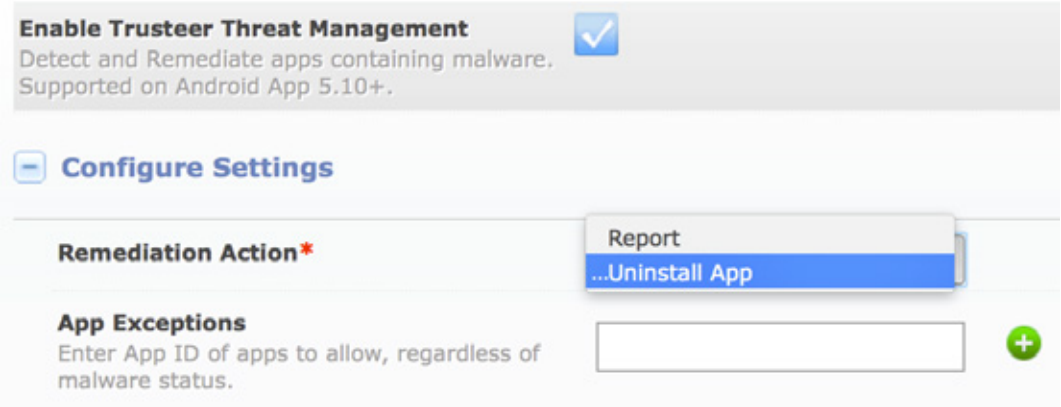

圖 4：某些 MaaS360 配置設定

補充破解或刷機裝置偵測：

- 偵測到遭破壞或脆弱的行動裝置
- 防範遭到破解的 iOS 和遭到刷機的 Android 裝置，這樣的裝置可為攻擊者提供作業系統的額外特權，造成各種攻擊向量
- 尋找隱藏者和現有的隱藏技術，這種技術會嘗試躲過破解和刷機裝置的偵測
- 套用無線更新的偵測邏輯，而不需要使用任何應用程式更新，就能更快回應花招百出的駭客
- 設定安全性原則和合規性規則以自動緩解
- 封鎖存取權，選擇性或完全抹除裝置或移除裝置控制

使用者的裝置和資訊也可以受到這層安全性的保護，但目前無法提供給消費者。

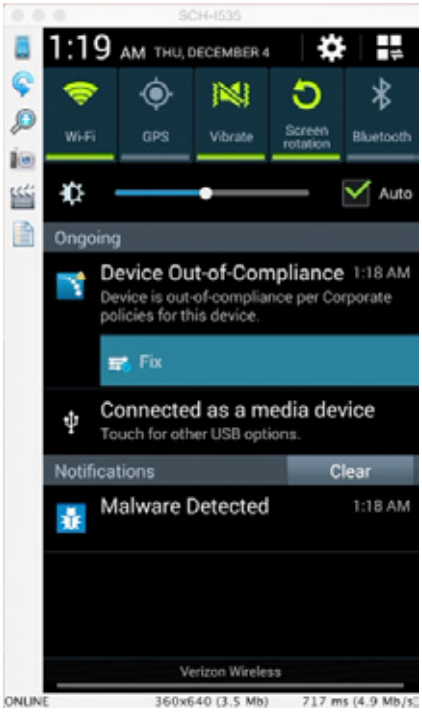

圖 5：螢幕擷取畫面顯示已偵測到行動惡意程式和裝置不符合規定

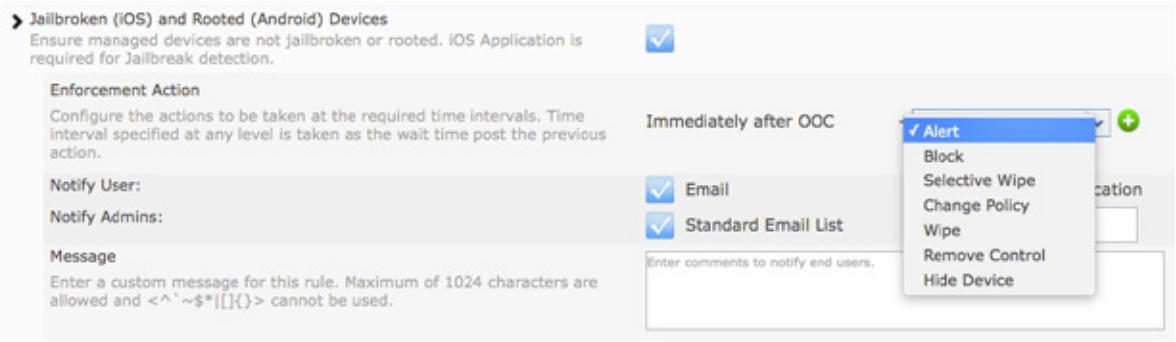

圖 6：針對破解和刷機裝置設定合規性強制執行動作

Trusteer Mobile Risk Engine 可啟用多層保護和網路犯罪智慧，以進行適應性惡意程式防範，從而快速偵測和因應最新攻擊行為，如此惡意程式就幾乎沒有任何機會來從事詐騙活動。持續更新以提供最新惡意程式，破解和刷機檢查，此引擎會根據裝置和應用程式風險因素，來執行近乎即時的行動風險評估。

主要優勢

MaaS360 Mobile Threat Management 解決方案的優勢不只能保護公司裝置及資料，使用者的裝置和資訊也可以受到這層安全性的保護，但目前無法提供給消費者。

組織可以做得更多來協助教育其使用者和保護其資料。

安全地支援 BYOD 和企業擁有的裝置

保護個人資料，可視為針對 BYOD 而另外增加的員工利益

近乎即時地主動管理行動威脅

降低企業和個人資訊之敏感性資料洩漏的風險

讓 Android 在企業中更普遍為人採用，特別是透過 BYOD

當行動安全性風險發生時，自動採取行動以補救

教育和保護使用者

除了這個 MaaS360 Mobile Threat Management 解決方案，組織可以做得更多來協助教育其使用者和保護其資料。

組織應該考量下列行動安全性活動：

- 教育員工關於應用程式安全性：教育員工關於下載協力廠商應用程式的危險，以及因為薄弱裝置授權可能產生的潛在危險。
- 保護 BYOD 裝置：套用企業行動力管理功能，讓員工能夠使用他們自己的裝置，同時還能維持組織的安全性。
- 只允許員工從授權的應用程式商店下載：只允許員工從授權的應用程式商店 (例如，Google Play，Apple App Store 以及您組織的應用程式商店) 下載應用程式。
- 裝置受到攻擊時，快速採取行動：在智慧型手機和平板電腦上設定自動化原則，在發現裝置受到攻擊或是發現惡意應用程式時自動採取動作。此方法可保護您組織的資料，同時可補救此問題。

為何選擇 MaaS360

有了 MaaS360：IBM 整合式進階惡意程式防護及領先業界的企業行動力管理和安全性方案，您就可以快速且簡單地設定和使用，以保護公司和個人行動裝置上的敏感性資料。

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

請回收

WGW03150-TWZH-01

1《在 2014 年全球行動電話數量將超過人口數量》，2013 年 1 月，國際電信聯盟，http://www.siliconindia.com/magazine_articles/World_to_have_more_cell_phone_accounts_than_people_by_2014-DASD767476836.html

2《行動應用程式安全性狀態》，2014 年 11 月，Arxan Technologies，https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

3 自攜裝置: 事實與未來， 2013 年 5 月，Gartner http://www.gartner.com/newsroom/id/2466615

4 Motive Security Labs 惡意程式報告，H2 2014，Motive Security Labs，http://www.gartner.com/newsroom/id/2466615

5《2014 年資料漏洞研究成本》：全球分析，2014 年 5 月，Ponemon Institute，http://www-03.ibm.com/security/data-breach/

6 《行動應用程式安全性狀態》，2014 年 11 月，Arxan Technologies，https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

7《行動應用程式不安全性狀態》，2015 年 2 月，Ponemon Institute，https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov33432&S_TACT=102PW2CW

8 IDC 全球季度手機追蹤報告，2015 年 2 月，IDC，http://www.idc.com/getdoc.jsp?containerId=prUS25450615

9《DroppedIn：Dropbox SDK for Android 中的遠端可利用漏洞》，2015 年 3 月，IBM Security，http://securityintelligence.com/droppedin-remotely-exploitable-vulnerability-in-the-dropbox-sdk-for-android/#.Vb-1_SisG8W

10《Wirelurker：OS X 及 iOS 惡意程式的全新時代》，部落格，PaloAlto Networks，2014 年 11 月 5 日；http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

11 Xue, H.，Wie, T.，Yulong, Z.；《Masque：您所有的 iOS 應用程式都是我們的》；Fire Eye，2014 年 11 月 10 日；https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html