IBM Security
創新思維領導白皮書

滿足 Android 愛好者

Android 甜點命名的更新是否改良裝置和資料安全性，而足以為企業提供服務？

IBM

Android 隨時可供企業使用。您的企業是否準備好要使用 Android？

簡介

長期以來，Android 一直引領消費市場潮流。現在，Google 和裝置製造商推出的最新安全性進展，以及領先業界之 EMM 解決方案提供者為 Android 提供的支援，都使得 Android 在企業界持續攻城掠地。為了協助確保符合業界標準及政府規範的安全性及合規性，企業需要一個方法來保護和管理全球最受歡迎之行動作業系統的眾多可用裝置、版本及特質。

這並非一體適用的情況。IT 必須檢查其裝置及應用程式範圍，然後決定自訂的企業行動力策略中有哪些安全性及管理功能是不可或缺的。透過 MaaS360® 等平台 (可讓您靈活運用 EMM)，企業可利用原生裝置及 OS 控制、資料容器化和雲端型擴充性，如此就能讓企業安心地使用 Android。

公司可讓員工使用其偏好或產業特定的裝置，但 IT 必須解決非常現實的疑慮，就是要如何保護公司資料和提供標準化的管理。

Android 幾乎無所不在：適用目的和附帶結果

Android 的全球行動裝置市占率高達 84%[1]，在全球超過 190 個國家/地區中掌控數億台行動裝置，用於工作和玩樂。這是任何行動平台的最大安裝用戶群，而且規模持續擴大。可供使用的 Android 裝置種類眾多，這代表它們通常非常適合公司的裝置資產方案。例如，許多在現場作業的員工需要堅固耐用的 Android 裝置，能夠防塵、防震、防雨、防濕、陽光輻射，以及承受極端的高度和溫度。有些人則是想要使用 Android 裝置的資料擷取功能，非常適合庫存控制和倉儲作業。

這個成長現象也衍生一些未預期的後果，以及 IT 的重要考量。公司可讓員工使用其偏好或產業特定的裝置，但 IT 必須解決非常現實的疑慮，就是要如何保護公司資料和提供標準化的管理。

全球最受歡迎的行動平台同時具有不穩定的安全性記錄；[2] 然而，Android 近期以甜點命名的 4.0 版 (Ice Cream Sandwich、Jelly Bean 和 KitKat)、5.0 版 (Lollipop) 和 6.0 版 (Marshmallow)，已經填補了過去最大的安全性弱點。在作業系統端，Android 4.0 支援加密功能 (一種適用於驗證管理的全新公開金鑰鏈架構) 以及保護功能 (可防禦像是記憶體入侵這種精密攻擊)。在 Android 5.0 中，會為使用者自動開啟許多重要安全性功能，包括鎖定螢幕、裝置加密和裝置管理員 (其有助於尋找和遠端抹除遺失的裝置)。Google 也已經要求 Security Enhanced Linux (SELinux) 的強制執行模式，基本上可限制應用程式及使用者的權限，以預防系統上的安全性缺口。若要針對企業環境啟用 BYOD，Android 5.0 中全新受管理的佈建程序可在裝置上建立受保護的工作設定檔。在桌面啟動器中，應用程式圖標會顯示一個工作徽章，以代表該應用程式及其資料是在工作設定檔內部受到 IT 管理員的管理。

您可以在統一檢視中看到個人和工作設定檔的通知。每個設定檔的資料會彼此分隔，兩個設定檔使用同一個應用程式時也是一樣。

Android 5.0 也針對手機和平板電腦提供訪客模式，而可讓您固定 (或鎖定) 應用程式，如此使用者就無法存取裝置的其他部分。這也是讓應用程式可在 Kiosk 模式中使用的絕佳方法，讓裝置得以在零售暢貨中心內展示。

Android for Work

顯而易見地，Google 聽到了企業的心聲和需求。當企業準備好啟動 Android for Work 時，Google 可讓 IT 具有容器化和企業級安全性控制能力。透過新的企業管理平台，Android for Work 可讓 IT：

- 區隔 Android 智慧型手機上的工作和個人資料
- 輕鬆管理和散發免費及付費的 Google Play 應用程式

Android for Work 將自動整合至 Lollipop，並且可供執行 Android 4.0+ 的任何裝置做為應用程式使用。

製造商：內建安全性及 EMM 整合

許多主要 Android 裝置製造商 (包含 Samsung、HTC、LG 及 Amazon) 也已經在最新裝置上實作企業級防護措施。有了內建功能，例如 SD 記憶卡遠端抹除和檔案加密、企業級 WLAN 安全性、VPN 存取，以及同時在一台裝置上支援公開和加密資訊的能力，讓許多 Android 裝置都更適合企業使用。

- Samsung KNOX 提供受保護的容器，讓您可以管理、維護和保護企業智慧。
- 獲 HTCpro 認證的裝置可提供政府等級資料加密，以及 VPN 和其他進階安全性功能。
- Amazon Fire 裝置具有加密、VPN、單一登入和認證註冊功能。
- 啟用 LG GATE 功能的行動裝置可提供進階的資安可管理性，還可支援增強型 Microsoft Exchange ActiveSync、資料加密和 VPN。

這四個和其他 Android 裝置製造商不僅啟用了關鍵安全性功能，也與領先業界的企業行動力管理 (EMM) 解決方案提供者發展合作夥伴關係。EMM 整合及 API 可讓企業透過單一入口網站，體驗穩健的管理及安全性功能。

最佳實務及能力

有鑑於 Android 第 4 和 5 版的廣泛安全性增強功能，IT 應該要求所有裝置都執行 Android 4.0 或更新版本且受到密碼保護。這可大幅降低分散和缺乏加密造成的「傳統 Android 風險」。雖然 Android 的靈活彈性讓企業 (及使用者) 對於一些最佳「量身訂作」裝置感到滿意，但這同時會造成曝露在危險下，IT 因此必須保護企業資料和實作防護措施，以抵禦刷機和行動惡意程式等攻擊。

危險的刷機：企業絕不接受的行為

使用者可以對 Android 裝置進行「刷機」，方法是存取其 UNIX 核心，而讓他們幾乎能夠安裝任何應用程式 (包含惡意程式) 並推翻應用程式層級的控制項。遭到「刷機」的裝置可能會讓公司網路曝露在已載入裝置的相同惡意程式下，並讓資料外洩防護功能失效。

資料遺失：企業就在您的口袋中

還記得美好的老時光嗎？要讓主力桌上型電腦曝露在這些攻擊下就難多了！今日，當資料在裝置之間移動時，非常容易遭到攻擊。具備卸除式 SD 記憶卡和 USB 連線的裝置可能很容易遺失資料，即使資料已經加密也一樣。在不安全的 Wi-Fi 區域中傳輸的資料也容易陷於風險，而且公司資料遺失或損毀可能面臨重罰，而且會喪失客戶信任及忠誠度。

行動惡意程式：無論是意外或蓄意為之，都很危險

在其「行動應用程式安全性狀態」報告中[3]，Arxan Technologies, Inc. 宣布 97% 的付費熱門 Android 應用程式和 80% 的免費熱門 Android 應用程式有時都會遭到駭客入侵。因為 Android 使用者可以從任何應用程式商店 (並非限於 Google Play) 安裝任何應用程式，所以與任何其他行動作業系統中的應用程式相較之下，會有較高比率的應用程式包含惡意程式，或是經過社群工程設計為連線至惡意程式。Arxan 發現「遭到破解的」行動應用程式會到處散播，因為有更多公司朝向以應用程式為中心的創新方向邁進，而且有更多員工會利用行動技術。

即使 Google Play 商店中原本應該無害的應用程式也可能會在您的網路和品牌中肆虐，因而可能導致收益損失、未經授權而存取關鍵資料、智慧財產權 (IP) 遭竊、詐欺，以及遭篡改的使用者經驗。例如，如果您的小孩拿了您的裝置並下載熱門遊戲 Temple Run，其程式碼便可存取您的根目錄檔案系統、下載快取或甚至是您插入裝置的 SD 記憶卡。它也可以透過裝置的麥克風來錄製音訊並追蹤您的所在位置。有了 IBM® MaaS360® 應用程式風險管理產品，您就能看到有關 Temple Run 的所有 (有些會讓您震驚不已) 應用程式安全性詳細資料。

為了防止此類漏洞，IT 必須知道已經安裝了哪些軟體、偵測行動惡意程式和遭到刷機的裝置、執行某層級的黑名單封鎖，並視需要強制執行合規性規則。

如何在 Android 環境中接近 EMM

無論裝置是公司或員工所擁有，許多 IT 部門都管理多種裝置類型、許多應用程式，而且可能還管理多個作業系統。

EMM 的最佳作法：自訂以準確符合您的環境和安全性原則。

IT 應該針對不同種類的使用者、部門、地理位置、裝置和應用程式進行「大小適中」的行動力管理投資，並套用最符合那些使用個案需求的技術方法。例如，銷售人員必須存取客戶聯絡及產品資料，而人資 (HR) 則會存取較敏感的資料，亦即在發生違規事件時，可能造成法規遵循責任的資訊。EMM 並非一體適用且不平等。

MaaS360 可協助滿足 Android 愛好者的需求

作為技術預覽合作夥伴，IBM 會與 Google 及製造商 (如 Samsung) 密切合作，以協助確保客戶能獲得最滿意的 Android 體驗。MaaS360 會直接與 Samsung KNOX 及 Android for Work 整合。使用 MaaS360，您就能以整合且穩健強大的方式來管理多種平台上的各種裝置。

藉由使用 Google、裝置製造商及 MaaS360 提供的功能，IT 可以存取廣泛的安全性選項和統一的平台，而可建立、管理和擴充分級式或分層式安全性方案。有了 MaaS360，您只需要部署自己需要的功能，利用環境中您需要的特定控制能力，選擇可讓您保護行動世界的個別解決方案。

MaaS360	您可以用它來做什麼
IBM® MaaS360® 行動裝置管理 您需要的裝置生命週期功能	• 控制存取權以及依需要隔離特定裝置或 Android OS 版本 • 強制使用密碼來保護傳輸中的資料、地理柵欄規則以及關聯式管理 • 偵測及限制遭到刷機的裝置 • 遠端尋找、鎖定和清除遺失或遭竊的裝置
IBM® MaaS360® 行動應用程式管理 如何打造智慧型行動企業	• 利用「容器化」保護企業應用程式 • 利用 Web 型主控台，集中管理行動應用程式 • 黑名單、白名單和設定必要應用程式以阻止資料洩漏和網路攻擊
IBM® MaaS360® 生產力套件 個別層級的一流防護	• 將個人資料和企業資料分開 • 在使用者層級設定個人角色原則 • 啟用線上和離線合規性檢查 • 抹除套件容器、應用程式容器、企業設定檔或整個裝置
IBM® MaaS360® 內容套件中建立、編輯、儲存和安全地共用內容 與控制協同作業	• 集中管理文件的散發，或是提供受保護的存取權以供存取現有的企業檔案儲存區 (例如，SharePoint、Windows 檔案共用、IBM Connections、Box、Google Drive、CMIS 以及許多其他來源) • 讓使用者在 Android 裝置上的加密容器中安全地檢視、建立、編輯和儲存所有文件 • 跨裝置類型 (包含 iOS、Android 及 Windows 裝置) 來同步內容
IBM® MaaS360® 閘道套件 保護您的入口通道	• 不需要裝置 VPN，即可讓受保護的行動裝置存取企業資料 • 賦予 SharePoint、Windows 檔案共用及內部網站行動能力 • 使用應用程式內 VPN 通道前往企業系統

MaaS360	其可提供何種功能
IBM® MaaS360® 行動威脅管理 在攻擊發生之前予以阻擾	• 利用持續更新的資料庫中的惡意程式簽章來偵測應用程式 • 啟用近乎即時的合規性規則引擎以自動進行修復 • 發現嘗試躲過刷機裝置偵測的隱藏程式
MasS360 應用程式風險管理 有助於從應用程式消除有風險的業務	• 透過深入、自動化的分析，識別數百個程式碼漏洞和有風險的應用程式行為 • 設計和測試應用程式規則，然後再針對業務單位、地理位置或工作群組進行部署 • 在使用者的裝置和企業應用程式商店上強制執行應用程式安全性原則

Android 已經正式可供企業使用，所以請與我們聯絡，以瞭解 MaaS360 如何協助您的企業使用 Android。保護您的公司資料，同時還能讓使用者在裝置上順暢地存取工作資訊。利用統一的原則、威脅管理、應用程式散發、裝置管理及標準架構，以便在各種 Android 裝置之間獲得一致的體驗。若要立即免費取得 30 天的 IBM MaaS360 試用版，請造訪：**ibm.com**/maas360.

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

1 「根據 IDC 的報告，全球智慧型手機在第二季貨運量超過 3 億個；而且 Android 及 iOS 兩者的全球市占率達 96%」，IDC Worldwide Mobile Phone Tracker，2014 年 8 月 14 日 (paywall) http://www.businesswire.com/news/home/20140814005599/en/Worldwide-Smartphone-Shipments-Edge-300-Million-Units

2 Ibid, 2014.

3 《行動應用程式安全性狀態》(研究報告)，Apps Under Attack，第 3 冊 (之前標題為：《應用程式經濟中的安全性狀態》)，2014 年 11 月 17 日，Arxan Technologies, Inc., https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美國印製 2016 年 3 月

WGW03108-TWZH-01