IBM Security
創新思維領導白皮書

行動資料安全性

保護機密資料同時保持行動使用者的生產力

IBM

行動資料安全性：尋找平衡

防止資料外洩 (DLP) 及「容器」等詞彙開始主導行動管理對話。在過去幾年，在提供工具和解決方案以便為行動裝置提供管理及安全性方面，已經有長足的進步；同時適用於企業擁有和員工自有的裝置。

一般而言，這些解決方案可符合保護裝置的需求，但它們缺乏常見於筆記型電腦及分散式網路部署的某些較精細的安全性層面。特別缺乏的是在筆記型電腦管理解決方案中常見的強大 DLP 控制項。

審慎的做法是去尋找其他更穩健的安全性控制項來補強行動裝置管理 (MDM) 解決方案，以協助保護敏感性資料以免被散發 (無論是不慎或惡意為之) 給未經授權的第三方。

利用具生產力、簡單的使用者體驗來平衡公司對於保護機密性資料相關風險的容忍度。

瞭解您的目標

研究技術時，您會探索不同方法。這些方法各有不同強項和弱點，但第一個工作是瞭解您的目標。發展出您的目標和方法概要時，您需要利用具生產力、簡單的使用者體驗來平衡公司對於保護機密性資料相關風險的容忍度。請務必考量下列事項：

阻止內賊 – 如果授權的使用者意圖複製資料，密碼原則及裝置加密是無法阻止他們的。控制這件事項屬於 DLP 的職責範圍。您的組織可能已經挹注大量投資以控制在筆記型和桌上型電腦之軟硬體周邊設備以外移動機密性資料。若是如此，請尋找可將 DLP 延伸至您行動裝置部署的功能。對於組織內的所有裝置類型，您的原則及目標都應該一致。

阻止外賊 – MDM 廠商社群已經完成了出色的工作，可提供用於保護行動裝置資料的工具。強制執行密碼及加密，以及能夠抹除裝置可說是已經完成了將近 90% 的工作。但是，能夠以一致和可靠的方式套用和驗證這些控制項仍然是存在的重要挑戰，特別是 Android 平台的各種機型。如果無法為所有裝置提供合理程度的保護，這個分散情況就會新增裝置多元性的這個面向。

廣泛、彈性的 BYOD 方案支援 – 裝置多元性是制定方法和策略的重大因素。畢竟，自攜裝置 (BYOD) 並不代表 *自攜 IT 核准的裝置*，這麼一來 BYOD 方案的精神就有點兒被打敗了。雖然裝置認證方案及
程序可提供某些結構，但完全開放的 BYOD 方案仍然需要某些先進技術的協助，以至少維持最低程度的資料安全性。

雙重角色是管理兩個獨立的使用者環境，以區隔行動裝置上的「工作」和「個人」資料及體驗。

雙重角色 – 這就是純粹安全性討論到其中一項功能和需要支援彈性 BYOD 方案的爭論分歧點。對於許多組織而言，他們並不需要穩健的 DLP 控制項，也沒有 DLP 控制項的政策。他們只希望不要接觸使用者的個人資料，但仍然必須能夠控制公司資料。將某些想法套用到您的目標時，雙重角色就可能是適合您組織的適當解決方案。基本上，雙重角色就是管理兩個獨立的使用者環境，以區隔行動裝置上的「工作」和「個人」資料及體驗。

其他考量 – 解決方案不會免費出現。確保您的 BYOD 方案能夠擴充、保持彈性且符合成本限制。您需要將使用者體驗納入考量，並確定使用者能夠接受和適應您實作的方案。您現在已經習慣民主的生活方式，沒辦法接受往日的 IT 獨裁風格了。

選擇您的方法

現在您已經將目標量化，讓我們來看看可用的方法。

容器 – 「容器」一詞似乎是用來描述提供區隔的工作應用程式及資料區之解決方案的最常見詞彙，有時候也常用「沙箱」一詞。您可能也會聽到將「雙重角色」用於描述此類解決方案，但應該將雙重角色視為目標，而不是解決方案 (例如，實作容器解決方案以達成雙重角色目標)。將這個方法視為完全區隔的「沙箱化」的區域，可在這裡進行特定活動並且移動資料僅限於沙箱內進行。因為所有工作活動都在此沙箱內進行，使用者將無法使用原生電子郵件用戶端，但能改為使用容器內部軟體提供的電子郵件、行事曆和聯絡人功能。這可能導致一些使用者不滿意，但如果實施正確，則能提供完美無縫的使用者體驗。重要的是協助您的使用者客群瞭解該解決方案的重要性，因為它協助組織達成其資料安全性的目標。

切分 – 這一種解決方案可攔截電子郵件資料流、切分相關內容 (例如附件、文字等)，然後在可控制資料流程的另一個應用程式中檢視及/或處理切分的內容。以電子郵件為例，使用者會與原生用戶端互動，直到他們需要存取的內容已經從電子郵件資料流移除 (切分)。移除的內容可能會儲存在執行「切分」的伺服器上，或是儲存在經過修改的行動端點上，而只能在安全的應用程式中開啟。

有了切分解決方案，就能分離使用者體驗。使用者會收到沒有文字和附件的電子郵件 (許多解決方案並不會基於此理由切分文字)，而可能必須啟動另一個應用程式，才能安全地存取文字和附件。

虛擬化 – 具體來說，這裡是指某軟體稱之為「Hypervisor」的技術，它會在行動裝置 (而非遠端伺服器) 上的軟體中實作「虛擬機器」。在這類型的解決方案中，企業可完全控制和管理虛擬裝置。所有公司應用程式和資料都會位於行動裝置上的虛擬機器內，在虛擬和實體裝置之間移動資料則會受到嚴密管控。基本上，這與 PC 和筆記型電腦的虛擬桌面基礎架構 (VDI) 相同，而且也會隨附許多相同的部署和管理挑戰。

如果您的組織是著重於阻止授權使用者從行動裝置散播機密性資料，則容器解決方案、虛擬化或電子郵件附件切分就非常有效。

這項技術也有其必備條件存在，就是裝置硬體及軟體的所有功能都要有可被虛擬化及受控制的可能性，就連網路連線能力及硬體功能也是。例如，在網路之間移動時，可虛擬化和虛擬變更 SIM (網路業者可能不喜歡這一點)。事實上，在行動裝置支援硬體內部的虛擬化之前 (類似於 PC 上的 Intel VT 和 AMD-V)，大規模普及還有很長一段路要走，特別是在 iOS 上。

以上皆非 – 塵埃落定之後，這可能是許多公司會採用的作法。如果您不屬於醫療保健或金融服務產業、沒有 PCI 或 HIPAA 法規要求，或是並未決定您的特定行動安全性需求及實作合理的裝置及應用程式管理策略，則對您使用者及 IT 所加諸的其他成本和複雜性可能不合理。

根據優先順序選取

現在讓我們根據您的優先順序加以對應

優先順序 – 內賊威脅： 如果您的組織是著重於阻止授權使用者從行動裝置散播機密性資料，則容器解決方案、虛擬化或電子郵件附件切分就非常有效。它們全部都能保護文字和附件，但在過程中基本上是提供不同的體驗，如上所述 (在切分的情況下，請審慎選取可同時提供文字及附件切分的產品)。如果沒有對電子郵件之任何資料外洩的彈性或容忍度，容器解決方案可透過提供改善的使用者體驗而獲得某些優勢，而且設定和管理起來較不複雜。理論上而言，虛擬化應該是適用於內賊威脅，但會產生實作和管理的挑戰。

優先順序 – 外賊威脅： 如果您對允許連線至電子郵件系統之裝置採取負責任的作法，就能妥善處理外賊威脅。如果您使用 MDM 解決方案
(假設您擁有此類解決方案) 以限制只有支援密碼原則、加密且可遠端抹除的受信任裝置能夠連線，則可能會外洩的資料以及因為裝置遭竊或遺失造成的相關損失就會有限 (如果不是為零)。如果您的優先順序是外賊威脅，您就可以省下 DLP 解決方案的額外成本及複雜性。一般而言，只有當其他漏洞已經堵塞住了，堵塞行動資料外洩漏洞才會生效。

容器解決方案可為位於不安全裝置上之公司資料提供安全區域，這也是升級使用者攜至方案之未認證或不適合裝置的替代方案。

優先順序 - BYOD 方案支援： 實作 BYOD 方案時，有一個審慎的步驟，就是制定裝置認證程序並建立允許的裝置清單，這樣可以提供基本的安全性等級。如果您已經實作方案，很快就會瞭解在 Android 的各種機型上支援關鍵安全性功能會有很大程度的差異。在完美的世界中，BYOD 可能代表能確實包容各式各樣的裝置。

容器解決方案可在不安全的裝置上提供一個安全的區域來存放公司資料，這也是一個替代方案，可用來升級使用者帶入方案中的未認證或不適合的裝置。假如切分解決方案可支援並可設定為能夠切分及保護電子郵件的文字和附件，那麼也可提供類似優點。因為可支援執行 Hypervisor 的裝置數量有限，所以虛擬化在支援廣泛的 BYOD 裝置方面沒什麼幫助。

優先順序 – 雙重角色： 另一個吸引人去實作容器或附件切分解決方案的動力並不完全是考量到安全性。隨著企業中的消費者裝置大量增加，公司和個人資料混雜也變成是不可避免的現象，雖然我們已經致力防止此情況。
為了採取比較親切而溫和的方法來處理這些裝置上的公司資料，也是一個關鍵動力。

不只是告訴使用者，如果裝置遺失、遭竊或是他們離職就會遭到完全抹除，還要讓他們知道可以選擇使用容器或切分解決方案。如此就可以自信地僅抹除公司資料，而不會影響使用者已經存放在裝置上的個人資料。容器方式能夠最有效地實現這個目標，而且採用恩威並濟的作法，可能是最理想的方法了。我們會將使用者引導至其「工作」角色，而且他們會對這樣的作法感到滿意，因為知道 IT 不會去觸碰他們的個人資料。

切分方法並不是很適合達成雙重角色的目標，因為如果原生電子郵件用戶端仍然用於個人和公司活動，則工作和個人資料之間並沒有明確區隔。

虛擬化也能提供美好承諾，但在裝置支援方面則有其限度，所以目前它並不是適合 BYOD 的實際替代方案。

三思而後行

總而言之，三思而後行。瞭解您的目標、瞭解您的使用者和瞭解可用技術及其對於環境和使用者的影響。更重要的是，在選擇廠商之前，先瞭解相關資訊。當您與廠商互動及使用解決方案試用版時，尋找可因應瞬息萬變行動環境的解決方案並時常重新評估您的目標。

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」的政策提供，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

WGW03113-TWZH-01