Ivanti UEM for Android

挑戰

- 保護Android設備上的敏感資料，同時維護用戶隱私。
- 確保用戶可以使用正確的應用程式。
- 組織內部缺乏科技專長，無法部署/擴展 Android 設備。
- 確認最正確的部署模式，傳遞具優越用戶體驗的關鍵商務價值給用戶。
- 提供跨Android設備一致性的管理，如Samsung, Pixel, Zebra等。

到處都是行動辦公室（Everywhere Workplace）

使到處都是行動辦公室成為可能。我們全面的統一端點管理（UEM）平臺是專門為保護Android 環境而構建的。輕鬆管理設備、應用程式和內容——經由我們的全球合作夥伴網路，可以在全球各地存取我們ＵＥＭ科技及整合性服務。

可擴展性、安全、容易、全球跨國的專業知識，這些只是組織信任Ivanti幫助他們加速採用Android的原因之一。憑藉每月25億台活躍設備，Android已經成為消費者的第一大行動平臺。對於企業來說，Android支持最廣泛的部署，包括單點使用、專用機、kiosk模式、一線員工的耐用設備和高端知識生產工具。

作爲第一個爲Android提供企業應用程式的商店、BYOD隱私控制和基於證書的身份管理的供應商，Ivanti也是首批支持Android企業平臺的UEM供應商之一。

作爲第一個爲Android提供企業應用程式的商店、BYOD隱私控制和基於證書的身份管理的供應商，Ivanti也是首批支持Android企業平臺的UEM供應商之一。

彈性應用

Ivanti UEM for Android支持廣泛的應用場景。按工作角色和設備所有權劃分用戶。公司所有、個人所有（BYOD）、知識型員工消費設備、任務型員工專用設備——使用Ivanti for Android，選擇最適合貴公司的產品，並使用適當的工具和設備來提高員工的生產效率，實現安全的行動轉型。

提供大規模跨設備一致性的IT管理

Android enterprise為企業客戶提供了更深入、更一致的安全模式。Ivanti支持這種模式。使用Ivanti的UEM控制台，IT部門可以安全地發佈企業應用程式，並將設定檔推送到Android企業設備。這些功能不僅簡化了IT管理，並藉由實現更一致的App派送及安全性，減少了Android的碎片化。

能力

- 藉由安全地啟用Android設備和應用程式來擴展多設備支持。
- 藉由整合Samsung Knox Mobile Enrollment (KME)及 Google Zero Touch Provisioning讓入職過程更為流暢及簡化。
- 在設備上區隔公務及個人資料 。
- 執行安全和隱私政策。
- 透過加密及DLP控制保護設備上的資料。
- 保留原生設備體驗，以維持員工滿意度。
- 在整個生命週期中保持組粒狀的應用程式級控制。

主要應用實例

- 保護企業機敏資料，確保企業內的隱私及合規性。保護任何端點上的業務資料以及各端點上的區隔公務及個人資料，包括Android 設備。
- 可在單一控制台同時管理跨設備,跨OS,及跨應用程式。在Android設備（包含Samsung,Google Pixel,Zebra,Oculus,Honeywell等品牌）,iOS,MacOS,及Win10設備同時存在的環境中，企業應將統一設備管理列為最優先。
- Android賦予一線工作人員更高的生產力 。醫療,車隊及製造業的現場,車隊及行動工作者可使用Android耐用型及Kiosk模式設備。提供卓越的終端用戶選擇和無縫的用戶體驗。設備選擇和用戶體驗對於生產效率和用戶合規性至關重要。Ivanti UEM提供了精簡的入職培訓和卓越的設備體驗。
- UEM的行業安全認證。獲得行業標準安全認證，如 FIPS 140-2 Validated Container、通用標準 MDM PP V3.0、DISA STIG、FedRAMP和國家密碼中心—— 具有高級別的認證。
- 為設備合規性提供安全自動化。自動合規性無需IT手動操作即可刪除受威脅設備上的所有業務資料。

企業Android的安全架構

Ivanti UEM for Android是如何很好地解決企業安全問題的？藉由區隔個人及公務應用程式及內容——同時保留原生使用者體驗。作為 BYOD程式的一部分，無論設備是公司所有還是員工所有，IT部門對企業容器有完全的控制。管理員可以設定和管理應用程式級和資料層級的策略，並對容器內的資料執行選擇性或完全抹除。

簡而言之：Ivanti UEM for Android為IT部門提供了全面的資料安全控制，同時用戶可在不同設備間保持無縫體驗。

設備安全

- 公司設備上的工作設定檔把使用者隱私保護的更好。
- 使用密碼策略保護Android設備，包括密碼管理。
- 通過鎖定設備存取來保護未經授權的存取。
- Kiosk模式鎖定，支持共享設備。

資料安全

- 單獨的應用程式資料加密。電子郵件、Wi-Fi和VPN使用以憑證為基礎的驗證方式。
- 安全單一登入。
- 選擇性抹除公務應用程式。

資料遺失防護（DLP）

- 附件加密控制
- 螢幕截圖控制
- 複製/貼上控制

保護網路存取

- Sentry作為郵件及線上內容閘道，可管理，加密及防護Android設備和後端企業系統之間的流量
- Tunnel是一個跨作業系統應用的VPN解決方案，允許企業授權特定的行動應用程式存取防火牆後面的公司資源，而無需使用者操作。

完整的設備生命週期管理

手動安裝Android設備是一項艱巨的任務。眾多的Android設備供應商如Google,HTC,LG,Samsung,Zebra,Honeywell等更讓此任務更具挑戰性。零接觸註冊(Zero Touch enrollment)結合Ivanti UEM，實現使用者（包含遠距員工）入職，用戶授權，設定檔，應用程式部署的自動化及Android端點安全控管。藉由零接觸註冊，貴公司亦可：

- 根據隱私/安全要求以特定模式提供設備。

使用公發設備？

使用Ivanti UEM for Android和零接觸維護安全性和原生使用者體驗。讓以下使用情境得以實現：

- 當使用者登入註冊設備時，自動進行使用者授權配置。
- 可部署企業內公發，Kiosk模式及單一應用App模式及共享設備。
- 集中配置及推送用戶電子郵件、Wi-Fi和VPN設定。
- 設定設備安全標準。
- 追蹤設備庫存及詳細資訊。
- 將公務應用程式無縫安裝到設備。
- 應用程式及Android更新自動化。
- 在設備生命週期結束、員工離職或設備遺失時清除設備上的公司資料。

Android 供應商零接觸註冊服務實例：

- Google Zero Touch Provisioning（ZTP）：讓IT管理人員可大規模部署配置及管理公發設備。
- Samsung Knox Mobile Enrollment (KME)：提供支援Android Enterprise(AE)的三星Galaxy設備具有自動註冊功能。

應用程式管理

行動應用程式是員工生產力的關鍵。這就是為什麼Ivanti為Android設備上的行動應用程式管理提供了最全面的平臺。Ivanti支援受企業管理的Google Play或Apps@Work，用於應用程式的發佈和探索，結合原生企業容器的資料安全或AppConnect和AppConfig，用於爲企業應用提供安全配置的行業標準方法。

藉由Ivanti for Android，公務應用程式被放在一個安全的容器中，資料經過加密和保護，防止未經授權的存取與抹除。單個容器密碼確保了對公務應用程式的存取，使用者可以輕鬆地在應用程式之間存取與共享資料。Ivanti為所有容器化的應用程式提供集中化策略管理，支持原生Android工作流程並爲使用者提供有生產力的行動體驗。

其他亮點包括:

- 透過Apps@Work私有應用商店提供安全、身份認證的企業開發和Google Play Store應用程式。
- 透過保護用戶應用程式提高生產效率：
  - Email+容器化企業電子郵件、行事曆和連絡人。
  - Docs@Work 用於安全的檔案儲存。
  - Help@Work 提供遠端控制，以便幫助服務人員更快地解決問題。
- 對Android設備上的公務應用程式和應用程式資料進行選擇性抹除。
- 允許/拒絕應用程式清單以防止不適當的存取。
- 容器化和動態策略可保護靜態數據，並透AppConnect實現基於應用程式且令人信服的使用者體驗。

Ivanti 統一端點管理

設備管理和安全	Secure UEM	Secure UEM Premium
安全和管理。保護和管理運行Apple iOS、macOS、iPadOS、Google Android和Microsoft Windows 10作業系統的端點。提供私有自建及雲端服務。	✓	✓
行動應用管理（MAM）。在派遣員工和員工設備上使用AppStation保護商業應用程式，而無需設備管理。	✓	✓
輕鬆入職。利用Apple Business Manager（ABM）、Google Enrollment和Windows AutoPilot等服務為使用者提供設動自動註冊功能。	✓	✓
安全電子郵件閘道。Sentry是一個線上閘道，用於管理、加密和保護行動終端和後端企業系統之間的流量。	✓	✓
應用程式分發和派送及配置。Apps@Work 是一個與Apple 大量採購計畫（VPP）相結合的企業應用程式商店，有助於行動應用程式的安全派送。此外，iOS管理的應用程式和Android Enterprise等功能允許輕鬆配置應用程式級別的設定和配置安全性原則。	✓	✓
安全連線	**Secure UEM**	**Secure UEM Premium**
Per-App VPN。Tunnel是一個跨作業系統應用的VPN解決方案，允許組織授權特定的行動應用程式存取防火牆後面的公司資源，而無需使用者操作。		✓
安全加密	**Secure UEM**	**Secure UEM Premium**
信任引擎。結合用戶、設備、應用程式、網路、地理區域等各種訊號，提供自我調整存取控制。		✓
無密碼用戶身份驗證。無密碼多因子且以設備做為身份認證，可應用在單一雲端服務或企業內部系統。		✓

Ivanti 統一端點管理(續)

擴展IT營運	Secure UEM	Secure UEM Premium
服務人員工具。Help@Work 允許IT在使用者允許的情況下遠程查看和控制使用者的螢幕，協助服務人員除錯及有效解決問題。	✓	✓
製作報表。透過客製化報表及自動調整動作，取得對所有受管理設備更具深度的資料與控管。	✓	✓
安全生產	**Secure UEM**	**Secure UEM Premium**
安全電子郵件和個人資訊管理（PIM）應用程式。Email+是一個跨平臺的安全PIM應用程式，適用於iOS和Android。安全控制包括政府級加密、基於證書的身份驗證、S/MIME、應用程式級加密和密碼強化。		✓
安全的網頁瀏覽。Web@Work藉由保護動態及靜態資料實現安全的網頁瀏覽。並可客置書籤及經由安全的Tunnel確保使用者可以快速及安全地存取商務資訊。		✓
安全的內容協同合作。Docs@Work 允許使用者可在資料儲存區（如Sharepoint,Box,Google Drive等）安全地存取，創建，編輯,標記,分享內容。		✓
行動應用程式容器化。部署AppConnect SDK或應用程式打包工具，為貴公司內部行動應用程式提供額外安全層防護，或自我們應用程式生態系統中選擇與AppConnect整合的App。		✓
額外認證功能。支援使用CAC，PIV的雙因子身份認證。		✓

關於 Ivanti

Ivanti使到處都是行動辦公室成為可能。在無所不在的行動辦公室內，員工可使用各種設備存取IT網路、應用程式和資料，讓員工無論在任何地方工作，皆能保持生產效率。Ivanti自動化平臺連結領先業界的統一端點管理、零信任安全和企業服務管理解決方案，爲企業提供了自我修復及自我防護設備能力和終端使用者自助服務的單一窗口。超過4萬名客戶，包括78家財富100強企業，選擇Ivanti來探索、管理、保護和服務他們的IT資產，從雲到邊緣，無論員工在哪裡用何種方式工作，皆能為員工提供最佳的終端使用者體驗。有關詳細資訊，請訪問 ivanti.com

ivanti

ivanti.com
+886 975-125148
ContactChina@ivanti.com