

趨勢科技

Trend Micro Mobile Security for Enterprises™

企業版行動安全防護 User Protection 使用者防護

趨勢科技 Mobile Security 行動安全防護是趨勢科技完整使用者防護當中不可或缺的一環，能讓您經由內建的單一主控台來完全掌握及監控行動裝置、應用程式和資料，在使用者生產力和 IT 風險之間取得巧妙平衡。

行動安全防護當中包含：

1. 行動裝置管理 (MDM)
2. 行動應用程式管理
3. 行動應用程式信譽評等服務
4. 裝置防毒 (Android)

趨勢科技 Mobile Security 行動安全防護是完整使用者防護策略的重要一環，相較於獨立分開的行動裝置防護與 MDM 解決方案，能大幅降低複雜性與成本，不需要建立新的管理基礎架構。

有別於其他解決方案，趨勢科技行動安全防護整合了多層式的防護來保護您的企業資料，不論資料移動到哪裡。藉由強制加密、遠端鎖定和清除、強制設定密碼等功能，再搭配裝置防護及應用程式管理，就能妥善保護您的資料安全。

防護點

支援以下作業系統的智慧型手機和平板：

- iOS
- Android
- Windows Phone



Securing Your Connected World

©2022年版權所有。趨勢科技股份有限公司及其相關機構保留所有權利。Trend Micro 與 t 字球形標誌為趨勢科技股份有限公司及其相關機構在美國或其他國家的商標或註冊商標。本文提及之第三方商標皆為其擁有人之財產。本文件內容若有變動，恕不另行通知。

威脅與資料防護

- 防毒
- 資料強制加密
- 強制設定密碼
- 遠端鎖定和清除
- 選擇性清除
- 行動裝置管理 (MDM)
- 行動應用程式管理 (MAM)
- 行動應用程式信譽評等服務
- 網站信譽評等

優勢

降低成本與複雜性

- 將行動裝置防護、MDM、行動應用程式管理以及資料防護集成單一解決方案來簡化管理。
- 利用趨勢科技 Cloud Communication Server 雲端通訊伺服器來簡化部署，這是一項選購的雲端服務，可將通訊自動化並降低部署的複雜性。
- 集中掌握與監控所有端點防護來降低營運成本。
- 藉由廣泛的平台支援來提高生產力與彈性。

提升掌握與監控

- 讓 IT 從單一主控台追蹤、監控及管理行動裝置、應用程式與資料。
- 掌握存取企業資源的裝置數量、類型與組態設定相關資料，不論裝置是否已登記。
- 藉由單一或多重伺服器集中建立並強制貫徹政策。
- 支援完整的使用者防護策略，與趨勢科技 Control Manager 集中管理主控台整合來將政策和管理與其他趨勢科技解決方案 (如 Apex One 端點防護) 集中在一起。

在科技與風險之間取得平衡

- 提供領先的病毒防護並確保裝置維持在最佳組態來降低惡意程式風險。
- 藉由遠端鎖定和清除以及選擇性清除來保護企業資料。
- 透過密碼和強制性政策來防止機密資料遭未獲授權者存取或不當使用。
- 讓 IT 利用趨勢科技行動應用程式信譽評等服務的雲端即時情報，來攔截危險的應用程式。



Securing Your Connected World

©2022年版權所有。趨勢科技股份有限公司及其相關機構保留所有權利。Trend Micro 與 t 字球形標誌為趨勢科技股份有限公司及其相關機構在美國或其他國家的商標或註冊商標。本文提及之第三方商標皆為其擁有人之財產。本文件內容若有變動，恕不另行通知。

主要效益

- 在員工方便性與 IT 控管之間取得平衡。
- 整合 MDM、行動裝置防護、應用程式管理以及資料防護於單一解決方案，降低部署以及 IT 和營運的成本。
- 採用以趨勢科技全球威脅情報為後盾的惡意程式防護、防火牆和入侵防護 (IDS) 來保護各式各樣的裝置。
- 利用加密、遠端鎖定和清除以及功能鎖定來保護資料，不論資料移動到哪裡。
- 提高員工生產力，讓員工隨時隨地都能工作，而且自由選擇自己喜歡的裝置。

主要功能

集中管理

- 利用趨勢科技 集中管理主控台來簡化管理，提供威脅防護與資料外洩防治政策的集中管理，涵蓋 IT 基礎架構的各個層面。
- 提供企業使用者的單一檢視，從桌上型電腦至行動裝置，按發生時間來檢視威脅，有助於發掘經由多重管道攻擊使用者的進階威脅。
- 提高政策貫徹的一致性，只需一鍵，就能將資料防護政策部署到端點、訊息、閘道等解決方案。
- 簡化裝置登記作業，可經由網站連結、QR Code 或 iTunes 下載。
- 提供立即的摘要檢視來查看所有裝置的違規狀況、裝置盤點、防護狀況以及健康狀況，不論裝置是否已登記。
- 掌握存取企業資源的裝置數量、類型與組態設定。

行動裝置防護

- 採用趨勢科技業界領先的惡意程式防護，以趨勢科技 Smart Protection Network™ 的雲端威脅情報為後盾。
- 可偵測並攔截惡意的應用程式與資料檔案。
- 利用網站信譽評等攔截惡意的網頁內容與網站。
- 利用防火牆與入侵防護 (IDS) 來防止裝置遭受來自網路應用程式、連接埠與服務的攻擊。
- 根據使用者政策來監控、攔截、記錄裝置所收發的電話、簡訊 (SMS) 與多媒體簡訊 (MMS)。



Securing Your Connected World

©2022年版權所有。趨勢科技股份有限公司及其相關機構保留所有權利。Trend Micro 與 t 字球形標誌為趨勢科技股份有限公司及其相關機構在美國或其他國家的商標或註冊商標。本文提及之第三方商標皆為其擁有人之財產。本文件內容若有變動，恕不另行通知。

資料防護

- 利用遠端鎖定和清除、選擇性清除或裝置定位，在手機遺失或失竊時保護企業資料。
- 強制貫徹資料加密與[法規遵循](#) (包括 [GDPR](#))。
- 在裝置越獄或未開啟加密時通知 IT 人員。
- 讓 IT 人員鎖定或或開放特定行動裝置功能，如：相機、藍牙、3G/4G 與 SD 讀卡機。
- 讓 IT 檢視未登記但仍存取企業網路的裝置。
- 讓 IT 在 Samsung Knox 相容裝置上部署、管理、設定 Knox 容器。

行動應用程式管理

- 透過應用程式拒絕名單和安全名單來防止連上網路的裝置使用未經核准或具風險的應用程式。
- 提供裝置盤點管理與報表，確實掌握裝置、群組與整個企業所使用的應用程式。
- 透過新的類別應用程式管理 (Category App Management) 功能，讓 IT 人員根據類別來管理、甚至封鎖特定類型的應用程式。
- 利用企業應用程式商店 (Corporate App Store) 功能將應用程式推播到使用者裝置，加快選擇性或必要性企業應用程式普及，應用程式商店甚至整合大量採購方案。
- 將已安裝的應用程式與趨勢科技行動應用程式信譽評等服務比對，偵測及攔截可能帶來安全與隱私權風險的應用程式。
- 支援 iOS 裝置大量採購方案的追蹤、管理及部署。

行動裝置管理

- 讓 IT 人員從遠端登記、配發或回收裝置的企業網路設定，如 VPN、Exchange ActiveSync 與 Wi-Fi®。
- 支援 Apple TV 和 AirPrint 服務部署 (針對 iOS 使用者)。
- 支援裝置定位與盤點管理來保護並追蹤企業持有或員工持有的裝置，不論裝置是否已登記。
- 提供跨裝置與群組政策，實行一致的安全與管理要求。

User Protection 使用者防護

趨勢科技 Mobile Security 行動安全防護是趨勢科技 User Protection 使用者防護多層式解決方案的一環，提供最廣泛且環環相扣的威脅防護及資料防護，範圍涵蓋端點、電子郵件、協同作業、網站以及行動裝置。



Securing Your Connected World

©2022年版權所有。趨勢科技股份有限公司及其相關機構保留所有權利。Trend Micro 與 t 字球形標誌為趨勢科技股份有限公司及其相關機構在美國或其他國家的商標或註冊商標。本文提及之第三方商標皆為其擁有人之財產。本文件內容若有變動，恕不另行通知。