產品型錄

Symantec Endpoint Protection Mobile for EMM
前身為 Skycure 行動裝置威脅防護

使用 SEP Mobile 的理由？

全面性的行動安全
多層式的行動防護，可抵禦所有攻擊媒介的已知、未知、目標式攻擊。

預測式技術
找出可疑網站與惡意開發者/應用程式，在其造成傷害之前即展開防護。

高產能且高效能
「Public」行動應用程式可協助保護隱私與產能，且不致負面影響行動體驗或電池使用時間。

輕鬆部署
快速用於原生的 iOS 和 Android 應用程式，並可輕鬆管理及維護。

企業等級
自動化的 IT 政策強制執行，可整合現有的企業 EMM/ MDM、VPN、電子郵件伺服器；且 SEP Mobile 可於數分鐘內部署至數千台裝置之中。[1]

高效率且清晰可見
優先呈現行動漏洞、威脅、攻擊行為等，更加上自動化的偵測與矯正功能。

龐大的群眾外包情報
透過完整且高效率的行動安全情報社群，以及賽門鐵克全球智慧型網路 (GIN)，抵禦零時差攻擊。

卓越的網路安全專業知識
SEP Mobile Research Lab 專責持續發掘並回報大量的漏洞與威脅，其中更為最近的四版 iOS 主版本回報並修正至少一個漏洞。

解決方案簡介

Symantec Endpoint Protection Mobile (SEP Mobile) 提供最完整、高效率、高精確度的 Mobile Threat Defense (MTD) 解決方案，提供更進一步的威脅情報，以預知並偵測更廣泛的現有或未知威脅。SEP Mobile 預測技術採用了多層方式，除了利用龐大的群眾外包威脅情報之外，更能同時用於裝置與伺服器架構的分析作業，不論是否為連網的情況下，均能主動為行動裝置抵禦惡意軟體、網路威脅、應用程式/作業系統漏洞攻擊。

強化您的 EMM 解決方案

SEP Mobile 直接整合全球最強大的企業行動化管理 (EMM) 解決方案。透過此整合特性，SEP Mobile 可添增行動威脅防禦的功能，進而延伸 EMM 的強大功能至先前無法觸擊的領域。如此能即時發現隨公共 Wi-Fi 與行動網路而來的威脅與攻擊、作業系統/應用程式的漏洞攻擊、惡意應用程式，以及因使用者行為而遭入侵的公司裝置與自攜裝置。

基於現今的駭客往往資金充裕且高度組織化，行動安全確實必須採用此種多層方式。最後，透過 SEP Mobile 與 EMM 之間的整合，您將可根據即時風險層級，透過政策強制執行而集中安全性與遵循管理。在目前以應用程式為基礎的資料導向時代，行動化可避免遭入侵的風險、可強化行動安全性分析，且精通過程毫無障礙。

SEP Mobile 目前已直接整合全球最強大的企業行動化管理 (EMM) 解決方案，包含：

vmware airwatch　Microsoft　CITRIX XenMobile

MobileIron　BlackBerry UEM　IBM MaaS360

解決方案要件

SEP Mobile 的企業級行動裝置威脅防禦平台，包含下列要件：

「Public」行動應用程式

- 易於部署、採用、維護，以及更新
- 毫不影響[2]生產力、體驗、隱私權
- 即時防護，避開特定的可疑網路與應用程式
- 遭受攻擊時，自動防護企業用戶的資產
- 對 SEP Mobile 的群眾外包威脅情報資料庫亦有所貢獻

雲端伺服器

- 對可疑應用程式的深入二次分析
- 信譽引擎具備應用程式、網路、作業系統所適用的機器學習功能
- 龐大的群眾外包威脅情報資料庫
- 透過 EMM、VPN、Exchange 及其他整合的政策強制執行
- 完整的活動記錄，適於統整任何 SIEM 解決方案

[1] 根據實際的客戶部署情況
[2] 根據客戶證言

防護廣度

防禦惡意軟體

- 主動抵禦零時差的惡意重新封裝應用程式
- 根據簽章、靜/動態分析、行為、架構、許可、資料來源等為基礎的漸進式應用程式分析
- 即時反應並防護多樣已知、未知、目標式的惡意軟體攻擊

網路防禦

- 有效的防護網可抵禦惡意 Wi-Fi 網路
- 偵測、阻絕、矯正惡意的 iOS 設定檔
- 專利的 Active Honeypot 技術不需影響隱私，即可識別出攔截式 (MITM) 攻擊、SSL 漏洞攻擊，以及內容操作攻擊

實體防禦

- 僅有 MTD 解決方案內建了 MDM 功能，並整合了現有的 EMM/MDM 解決方案
- 萬一裝置遺失或遭入侵，亦可遠端清除
- 密碼鎖定可保護企業資訊
- 自動升級/更新至 SEP Mobile 應用程式與設定檔
- 針對裝置、使用者、群組製作全方位報告

漏洞防禦

- 監控未修復的已知漏洞
- 教育使用者並提醒 IT 資安人員
- 發現應用程式與作業系統中的零時差漏洞，並同時知會廠商
- 偵測未知與已知的漏洞

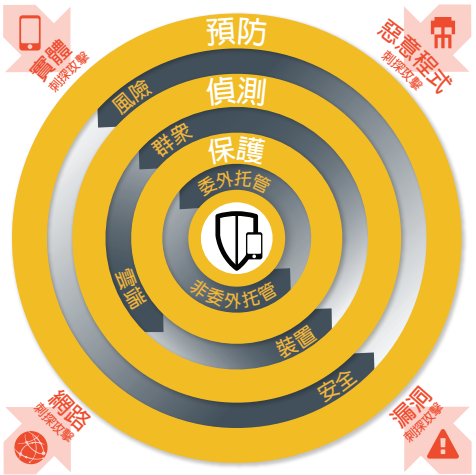

圖 1：SEP Mobile 多層式安全技術

情報深度

裝置

- 第一線防禦，找出可疑的應用程式與網路
- 根據多樣特性，對應用程式進行漸進式分析
- 立刻找出可疑和不合法的網路
- 根據風險資料庫，交叉比對裝置類型、作業系統版本等等

雲端伺服器

- SEP Mobile Research Labs 時時站在駭客角度思考，以搶在駭客之前行動
- 深度靜態與動態分析，包含以機器學習為基礎的行為分析
- 持續監控並評估漏洞的嚴重性
- 由其他企業系統所提供的情報 (即 EMM、SIEM)

群眾

- 全球的所有 SEP Mobile 應用程式，均是感應器與資料蒐集器
- 同時由好、壞應用程式與網路提供的特性目錄
- 評估作業系統版本與裝置類型，決定升級與否
- 對重新封裝的應用程式與其他惡意軟體而言，零時差偵測特別重要

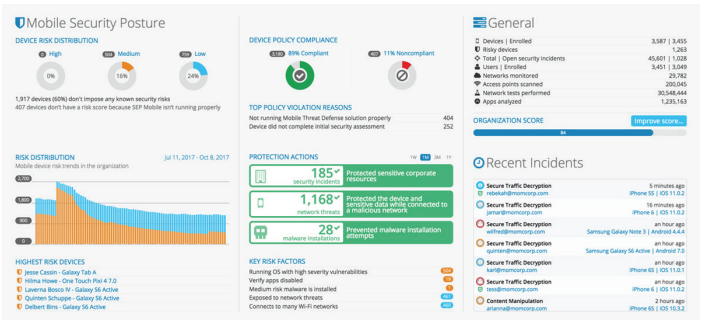

圖 2：SEP Mobile 管理主控台

免費試用*

透過試用與風險評估，讓自己的企業得以一瞥目前所面臨的所有威脅。五分鐘以內即可安裝完畢並開始執行。開始免費試用 ›

* 需遵守此處適用的條款與條件。

Symantec + Skycure

台灣賽門鐵克股份有限公司
地址：台北市信義路五段 7 號台北 101 大樓 13 樓 A 室 |
電話：(02) 8726-2000 | 傳真：(02) 8726-2199 | www.symantec.com/zh/tw

SYMC_DS_Endpoint_Mobile_EMM_TW_v1