CHECK POINT SANDBLAST MOBILE

優勢

- 放心地在組織網路上部署任何 iOS 或 Android 行動裝置
- 保護行動裝置上的敏感資訊免遭窺探
- 藉助可輕鬆整合到現有行動和安全基礎設施 (MDM、MAM、NAC、SIEM 等) 的行動安全機制，提升可視性並加大保護，以利防禦最新的行動威脅
- 強化 Microsoft Exchange 和容器/包裝解決方案的安全措施
- 能夠針對跨平台的進階持續性威脅 (APT) 攻擊做出快速回應
- 能夠讓約聘人員安全地從未受管理的裝置存取企業資料
- 保護使用者體驗和隱私權，同時增加組織所需或法令規定的防護能力

先一步偵測並阻擋攻擊

智慧型手機和平板電腦給我們前所未有的機會，讓我們可以隨時隨地存取所需的重要業務資訊，以提高工作效率和精準度。讓員工在所選行動裝置上存取重要業務資訊有許多好處，但也會使公司身陷風險之中。

Check Point SandBlast Mobile 採適用於 iOS 和 Android 裝置的創新行動安全方法，可先一步偵測並阻擋行動威脅攻擊。不論您的資料是留存在裝置內還是透過雲端移動存取，SandBlast Mobile 都可保護您免於承受使資料處於風險之中的漏洞和攻擊。

適用於企業的最高等級行動安全

只有 Check Point 可提供全面的行動安全解決方案，以保護裝置免受侵入裝置 (作業系統)、應用程式、網路以及 SMS 訊息的威脅攻擊，從而提供業界最高的 iOS 和 Android 威脅攔截率。SandBlast Mobile 透過套用威脅模擬、先進靜態程式碼分析、應用程式信譽和機器學習等方式，使用惡意應用程式偵測功能來發現已知和未知的威脅。

其可保護裝置免遭未受保護的 Wi-Fi® 網路存取及中間人攻擊，並在偵測到威脅時阻止對企業網路的存取。它透過偵測攻擊、漏洞、設定方面的更改及先進的改機和越獄行為，在裝置層級 (作業系統) 使用即時風險評估機制，以利縮小攻擊範圍。另外，其動態威脅回應功能可防止遭到入侵的裝置存取組織的網路，並允許組織依據裝置上獨特的威脅補救和排除閾值，設定彈性原則控制項。

先進的應用程式分析

您可以信任員工並允許他們存取您的敏感企業資產，但您能夠信任他們的應用程式嗎？SandBlast Mobile 可在應用程式被下載至裝置時將其擷取，並在虛擬的雲端式環境下執行各個應用程式，以在被核准或標記為有惡意之前分析其行為。簡單易懂的可匯出分析報告，有助您的安全團隊確保員工所使用的應用程式安全無虞。

網路式攻擊

公共場所充滿無安全保護的 Wi-Fi 網路，因而難以得知哪些網路是安全的，哪些網路存在風險。網路犯罪份子可利用這些網路入侵智慧型手機和平板電腦，從而取得裝置及寶貴資料 (如訊息、檔案及網路憑證) 的控制權。SandBlast Mobile 偵測惡意網路行為和狀況，並自動停用可疑網路，以確保裝置和資料的安全。

2017 年 4 月 20 日

裝置漏洞評估

網路犯罪份子的目標是先一步發現您安全機制中最脆弱的環節；這通常包括其他安全解決方案可能無法偵測到的作業系統和應用程式弱點。我們的解決方案會持續分析裝置，以發現網路犯罪份子用以攻擊裝置和竊取資訊的漏洞與行為。我們提供針對行動裝置所面臨威脅的更佳可視性，協助您縮小整體攻擊範圍並降低相關風險。

簡訊釣魚攻擊

簡訊釣魚攻擊又稱為 SMiShing (簡訊釣魚)，是一種詐騙形式，其中攻擊者透過在簡訊中偽裝成信譽良好的實體或人物，嘗試取得登入憑證或帳戶資訊等資訊。受害者會收到看似由已知聯絡人或組織發送的 SMS 簡訊。訊息中的連結可能在使用者的裝置上安裝惡意軟體，或將使用者導向惡意網站環境，以誘騙他們透露個人和財務資訊，如密碼、帳戶 ID 或信用卡詳細資料。該解決方案偵測惡意簡訊並加以封鎖。SandBlast Mobile 防簡訊釣魚攻擊技術由 ThreatCloud™ 提供支援，這是業界最大型的協作網路及雲端驅動知識庫，可提供即時、動態的安全情資。

完整行動威脅可視性與情資

SandBlast Mobile 的雲端式儀表板讓支援裝置的管理和行動威脅的控制作業變得快速又簡便。其可為您的安全和行動團隊提供即時威脅情資，並提供可能影響企業或使用者之行動威脅數量與類型的詳細資訊。

將情資與現有系統兩相整合

SandBlast Mobile 的即時威脅情資流推動 Check Point SmartEvent 自動監控安全事件，並與內部網路攻擊產生相互關係。此資訊在 Check Point 的 ThreatCloud™ 內共用並產生關聯，從而提供可在網路環境內使用的最廣泛威脅情資，以利進一步避免網路攻擊的發生。也可將威脅情資匯入現有企業系統，如您的安全資訊及事件管理 (SIEM) 平台。這包括可進行過濾以觸發回應動作的詳細記錄和其他受駭指標，這些動作會協助您的安全團隊快速採取行動，以控制並消除風險。

行動安全部署從未如此簡單

安全和行動團隊所需煩憂之事已經夠多；這也正是我們設計 SandBlast Mobile 的原因，透過與 MDM 或 EMM 解決方案的整合與搭配，幫助他們快速並放心地保護行動裝置的安全。這不僅有助提高解決方案的可縮放性，還提供在更廣大安全基礎設施中管理行動安全的強大運作和部署效率。

輕鬆部署先進的行動安全機制

不論您支援 300 台或 300,000 台裝置，都可快速又簡便地將 SandBlast Mobile 與您的 EMM 相整合。透過 EMM 即可自動部署和管理，從而加快採用速度並降低整體運作成本。此解決方案可依您的 EMM 相應調整，以利無縫保護納入防護範圍的行動裝置。因此，您可確信自己擁有管理和保護行動裝置所需的安全層級，即使是在變化多端的環境下亦可高枕無憂。

直接在裝置上採取補救措施並消除威脅

識別出威脅時，SandBlast Mobile 會自動針對風險採取補救措施，直至消除威脅。若可立即在裝置上消除威脅，系統會通知並提示使用者採取行動，如刪除惡意應用程式或中斷與惡意網路的連線。與 EMM 整合後，此解決方案可限制安全容器存取，或在受駭裝置上進行即時的風險式原則調整，而 EMM 無法自行執行這些作業。SandBlast Mobile 也會啟用隨需 VPN，另外導出資料流量以避開網路犯罪份子並避免資料擴散，同時仍讓使用者維持連線狀態。

重視使用者隱私及裝置效能

一般使用者的隱私非常重要，因此 SandBlast Mobile 絕不分析檔案、瀏覽器歷史記錄或應用程式資料。此解決方案會使用來自作業系統、應用程式和網路的靜態和內容中繼資料，以判斷裝置是否受駭；並會將用於分析的資料匿名處理，從而將之與安全情資資訊分開。分析作業在雲端執行，以免影響裝置效能，而且由於防護作業在背景執行，所以使用者無需學習新功能即可受到保護。

詳情請瀏覽 checkpoint.com/mobilesecurity

聯絡我們

全球總部 | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | 電話：972-3-753-4555 | 傳真：972-3-624-1100 | 電子郵件：info@checkpoint.com

台灣分公司 | 臺灣臺北市大安區信義路 4 段 6 號 6 層 | 電話：886-2-2703-2798 | 傳真：886-2-2703-2796 | www.checkpoint.com