VMware Carbon Black App Control

僅允許執行受信任軟體的主動式安全性模式

使用情境

- 鎖定地端、私有雲或公有雲中的系統
- 保護具備固定功能的裝置
- 保護生命週期已結束 (EOL) 的作業系統
- 保護進行氣隙處理的系統

優勢

- 防範惡意軟體、勒索軟體與新一代攻擊
- 縮短重要系統的意外停機時間
- 整合端點代理程式
- 預防對系統設定進行惡意變更
- 滿足重要法規命令的 IT 與稽核控制規定
- 透過簡化的 IT 稽核流程來提高 IT 資源的效率
- 為執行生命週期已結束之作業系統的舊版系統提供保護
- 識別重要環境中的所有軟體
- 避免將資料寫入未批准的裝置

隨著安全性威脅和惡意軟體不斷進化，抵禦這些威脅的技術也需與時俱進。畢竟，企業往往無法承受因安全性漏洞造成意外停機或效能衰退，而衍生的生產力損失、信譽損失，以及成本損失。鑑於此一態勢瞬息萬變，各方皆積極尋求以下問題的解答：隨著伺服器和端點威脅的數量不斷增加，且目標更加明確，最佳因應之道究竟為何？

安全性方法可劃分為主動式和被動式兩大類別。多年來，講求偵測和抵禦已知惡意事件的被動式安全性，持續提供特定層級的安全性保證。封鎖已知病毒、蠕蟲和其他惡意事件特徵的功能，協助許多系統免於遭到入侵。然而，新型態攻擊的發展，已大舉超越被動式安全性模式的守備範圍。但這並不表示被動式安全性模式應遭到淘汰，事實上，此舉仍屬必要之舉，卻不足以獨撐大局。

主動式安全性模式可識別軟體的已知信任等級，且僅允許存取受信任的資源。主動式安全性模式會假設未知軟體不受信任，並要求先行指派信任，再授予存取權限並允許使用。典型的主動式安全性模式，只會提供已知良好的要求和結果。

VMware Carbon Black® App Control™ 可運用主動式安全性模式，保護位於地端、私有雲或公有雲中的關鍵系統。如此一來，就能防範惡意變更，並確保持續符合法規要求。

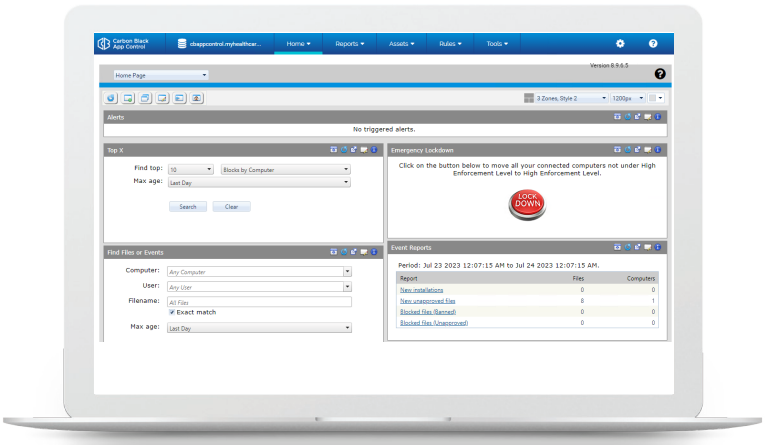

圖 1：鎖定位於任何地點的系統，以防範惡意變更

功能

- 應用程式控制
- 檔案完整性監控與控制
- 裝置控制
- 記憶體保護
- 登錄保護
- 應用程式目錄監視清單
- 通用平台列舉
- 快速設定
- 內容式檢查
- 流程掏空保護

平台

感應器支援：

- Windows XP、Server、Embedded、POS
- Mac OS X
- RHEL Linux
- Oracle RHCK Linux

全方位的主動式安全性方法

VMware Carbon Black App Control 會藉由納入以下功能，以採取全方位的主動式安全性方法：

- 應用程式控制 (允許清單和拒絕清單) 會提供多種控制層級，以控制應用程式與系統資源互動期間可進行的操作。
- 檔案完整性監控 (FIM) 會檢查主機作業系統內敏感檔案、登錄金鑰和資料夾的完整性，並檢查檔案是否遭到變更或竄改。檔案完整性控制 (FIC) 則會回報或封鎖變更。
- 裝置控制會提供完整的控制能力，以定義或限制來自外部儲存媒體 (例如 USB) 的資料傳輸。只要實作一系列的存取規則，企業就能設定多個參數，以授予或限制特定裝置、使用者或群組在排程時間內的連線。
- 記憶體保護會控制記憶體的存取權限。記憶體保護的主要目的，在於避免流程存取未配置給自身的記憶體。
- 登錄保護會避免 Windows 上的系統關鍵登錄金鑰遭到修改。而此舉正是防止登錄金鑰遭到攻擊的必要措施，原因在於，如果重要金鑰遭發生損毀或遭到修改，即有可能造成無法逆轉的傷害。Carbon Black App Control 可回報或封鎖變更。

靈活的部署

隨著 IT 和安全性部署作業逐漸移轉至雲端，若未持續留意目前容易存在漏洞的領域，就有可能導致安全性落差。但矛盾的是，許多公司依舊將關鍵系統和資料存放在進行氣隙處理的伺服器上，或是所執行作業系統已屆生命週期的系統上。無論在資料中心內，或是在 Amazon Web Services (AWS)、Microsoft Azure 或代管私有雲上，Carbon Black App Control 都能提供主動式安全性方法。而僅限雲端的安全性方法，將無法保護：

- 與網際網路和 Carbon Black App Control 伺服器中斷連線的氣隙處理系統
- 具備固定功能的裝置，例如提款機、銷售點系統、Kiosk 和醫療裝置
- 已屆生命週期的作業系統，例如 Windows XP 以及 Windows Server 2003 和 2008
- 使用專用軟體和資料，且視為公司命脈的關鍵系統

若要取得更多資訊或購買 VMware 產品

請致電 +886-2-3725-7000、造訪 vmware.com/tw/products 或線上搜尋授權經銷商。

請為貴企業安排個人化示範。

請造訪 VMware Carbon Black App Control 產品頁面。

受信任的內容核准

Carbon Black App Control 並不會維護檔案清單或資料庫，畢竟，這些項目往往容易過時。相較之下，Carbon Black App Control 會採用以信任為基礎的方法來進行內容核准，當中涵蓋多個機制，可在無需維護核准雜湊清單的情況下進行檔案核准。如此一來，就能更輕鬆地實現主動式安全態勢。當中包括：

- IT 和雲端導向的信任 - 從雲端提供受信任的目錄和威脅 / 信譽。
- 受信任的發佈者 - 允許企業選擇信任 Google、Adobe、VMware，或其所信任的其他來源。
- 自訂規則 - 提供更精密的控制，以允許依路徑、流程和使用者來核准檔案。
- 外部資源 - 使用事件規則功能傳送全新 / 未知檔案，以進行靜態或動態分析，然後根據分析結果來加以核准或禁止。

摘要

VMware Carbon Black App Control 可鎖定您的環境、防範惡意變更，並確保持續符合法規要求。Carbon Black App Control 採用主動式安全性模式，可啟用預設 / 拒絕安全態勢，以持續抵禦可規避傳統安全性防護措施的網路威脅。

Carbon Black App Control 並不會維護檔案清單或資料庫，畢竟，這些項目往往容易過時。相較之下，當中會採用多個核准方法，包括 IT 和雲端導向的信任、受信任的發佈者、自訂規則和經驗證的外部資源。

VMware Carbon Black App Control 可讓您無後顧之憂。

文件編號：2170550aq-ds-nsx-A4-102-proof 10/23