VMware Carbon Black Cloud

Enterprise EDR

搜尋威脅與事件回應

使用情境

- 搜尋威脅
- 事件回應
- 警示驗證與分級處理
- 根本原因分析
- 鑑識調查
- 主機隔離
- 遠端修復

優勢

- 降低複雜性，以提供更有效率的端點安全性
- 容易部署、自動更新、具備彈性延展性
- 透過持續掌握端點能見度加快調查速度
- 完整瞭解根本原因，以弭平現有落差
- 為調查提供安全的遠端存取
- 大幅降低停留時間與解決問題所需的平均時間

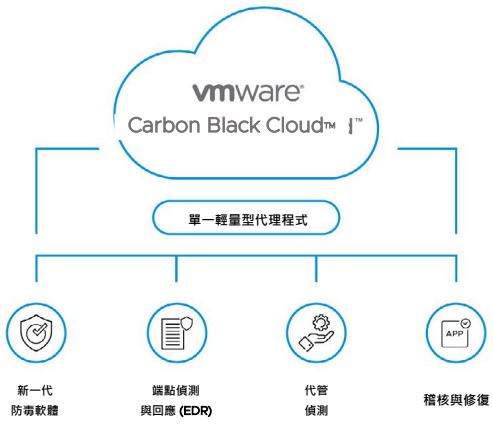
為了能取得所需端點資料以進行調查，並主動搜尋異常行為，企業安全性團隊總是疲於奔命。目前，安全性與 IT 專業人員不僅難以釐清可疑活動背後的真相，也需要尋求可深入分析資料的方法，以便做出判斷。

VMware Carbon Black Enterprise EDR 是一款能夠搜尋威脅並回應事件的進階解決方案，持續為頂尖安全性作業中心 (SOC) 與事件回應 (IR) 團隊提供能見度。Enterprise EDR 將透過新一代端點保護平台 VMware Carbon Black Cloud 提供，此平台能使用單一代理程式、主控台與資料集來整合雲端的安全性。

運用持續收集並傳送到 VMware Carbon Black Cloud 的資料，Enterprise EDR 就能隨時讓使用者立即掌握最完整的攻擊狀況，將調查事件所需的時間從幾天縮短到只要幾分鐘。如此一來，團隊就能主動搜尋威脅、找出可疑行為、中斷主動攻擊，並在攻擊者能針對漏洞出手前就解決漏洞。

Enterprise EDR 也能持續提供能見度，讓您擁有立即回應並修復的能力，攔阻主動攻擊並迅速修補損害。

雲原生端點防護計畫



「Enterprise EDR 能夠快速探索單純與進階威脅，大幅簡化事件回應的過程。這樣的簡化程度與回應能力實在讓人驚嘆，尤其是當調查行動分秒必爭時…維護端點安全性原本是個艱難任務。」

MIDCAP FINANCIAL SERVICES IT 系統安全性工程師 DENIS XHEPA

功能

- 輕量級感應器，可在雲端部署與管理
- 可處理集中化的未篩選資料，並進行二位元搜尋
- 現成且可自訂的行為偵測
- 專屬第三方威脅情報摘要
- 自動化執行儲存區觀察清單查詢
- 將互動式且可延展的攻擊鏈視覺化
- 適用於快速修復的安全遠端 shell
- 開放式 API

平台

- Windows
- macOS
- Red Hat
- CentOS

深入瞭解

如需安排個人化示範，或於組織內免費試用，請造訪 *CarbonBlack/trial*

若要取得更多資訊或購買 VMware Carbon Black 產品，請致電 +886-2-3725-7000

如需詳細資訊，請將電子郵件寄送至 *Contact@CarbonBlack.com* 或造訪 *CarbonBlack.com/epp-cloud*

主要功能

完整端點保護平台

Enterprise EDR 建構在 VMware Carbon Black Cloud 上，能從相同的代理程式與主控台提供進階威脅搜尋與事件回應功能，做為新一代防毒軟體、端點偵測與回應和即時查詢解決方案，讓團隊能在融合式平台上整合多個端點的產品。

不間斷且集中化的記錄

由於能夠集中存取不間斷收集的資料，安全性專業人員可以取得所有需要的資訊，以便即時搜尋威脅，並於漏洞出現後進行深入調查。

將攻擊鏈視覺化並進行搜尋

Enterprise EDR 提供直覺的攻擊鏈視覺化功能，可快速輕鬆的識別根本原因。分析人員可迅速概覽每個攻擊階段，以洞悉攻擊者行為、消弭安全性落差，並且從每一個新的攻擊技巧汲取心得，以防二度受害。

透過 Live Response 來遠端修復

有了 Live Response，事件回應者就能隨處建立安全連線，以連接受感染主機，進而提取或推送檔案、關閉流程、執行記憶體傾印，並迅速進行修復。

透過整合與開放式 API 進行自動化

Carbon Black 坐擁強大的合作夥伴商業網路，並採用開放式平台，可讓安全性團隊將 Enterprise EDR 等產品整合至現有安全性堆疊中。

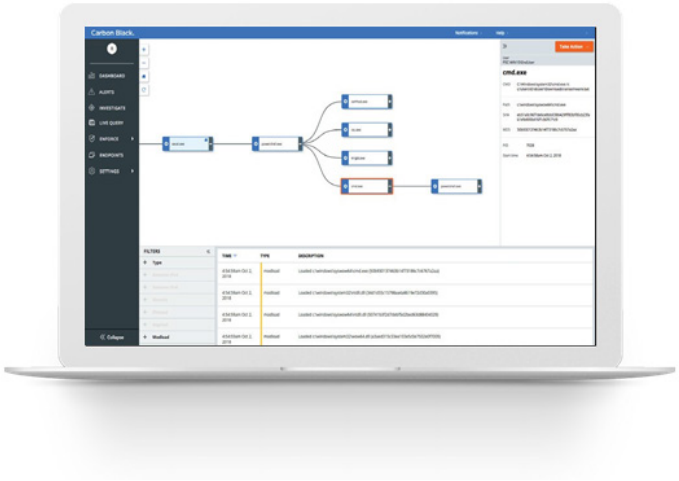


圖 1：企業端點偵測與回應會運用持續收集的端點活動資料，將廣泛的攻擊鏈視覺化，讓使用者清楚瞭解攻擊的每個階段究竟發生了什麼事。

vmware Carbon Black