VMware Data Retention™ for VMware Carbon Black Cloud™

提升事件資料儲存空間

使用情境

- 增加在單一平台上管理事件的時間
- 具備更多歷史資料來因應事件
- 偵測為期更長、速度較慢的攻擊手法

優勢

- 推動更有效率且主動的安全性作業
- 從事件關聯中提供更多情境脈絡
- 透過持續掌握端點加快調查速度
- 消除需將事件移轉至協力廠商工具的額外負荷
- 降低增加的資料事件儲存空間成本
- 能更清楚查看安全性趨勢

VMware Data Retention VMware Carbon Black Cloud

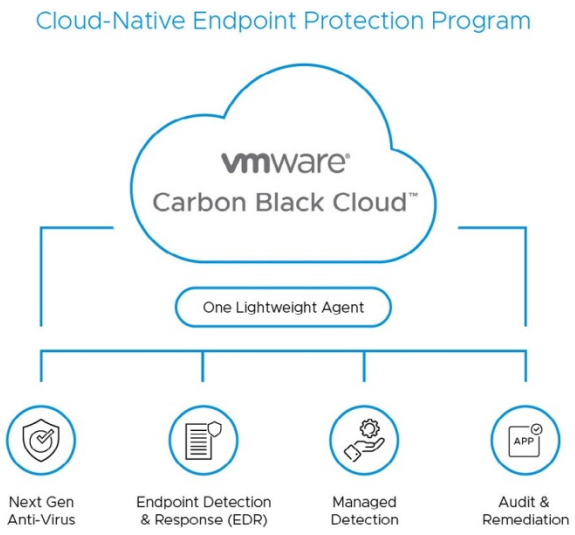
- 事件在 VMware Carbon Black Cloud 平台上可以儲存 60/90/180 天

隨著企業的安全性堆疊變得日益複雜，要找出漏洞並加以應對，平均得花上 150 天，主要原因在於缺少歷史資料。為了有效處理漏洞，您必須能夠回顧過往，取得更長一段時間的資料。

VMware Data Retention for VMware Carbon Black Cloud 讓組織只需動動指尖，就能快速、有信心地以更多的事件資料進行調查。

VMware Carbon Black Cloud 是新一代端點保護平台，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，而 VMware Data Retention 會以平台附加元件的形式提供至 VMware Carbon Black Cloud。

運用持續收集並傳送到 VMware Carbon Black Cloud 的資料，新一代防毒軟體和企業端點偵測與回應模組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。現在，企業有更多時間可以分析並利用這些資料來強化團隊，主動搜索威脅、發現可疑行為、中斷進行中的攻擊，並在攻擊者找到防禦漏洞之前加以解決。



平台

VMware Data Retention 是 Carbon Black Cloud 的附加元件服務，支援：

- Windows 7 與更新版本
- Windows Server 2008 R2 與更新版本
- MacOS 10.10 與更新版本
- RedHat 6 與更新版本
- CentOS 6 與更新版本
- Ubuntu 16.04 與更新版本
- SUSE 12 與更新版本
- OpenS USE 15 & 42
- Amazon Linux 2

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，請傳送電子郵件至 *Contact@CarbonBlack.com*，或造訪 *CarbonBlack.com/epp-cloud*

主要功能

快速準確地進行調查

在正確時間存取正確資料，縮短 MTTR (平均解決時間)。能查看更長一段期間的事件和取得相關脈絡，意味著您可以進一步回顧過往資料並瞭解整條攻擊鏈，進而調查整起攻擊。這麼一來，安全性分析人員就能回答「究竟發生什麼事情」、「在哪裡發生」以及「如何快速解決」等關鍵問題。

更有信心搜尋威脅

運用 VMware Carbon Black Cloud 上企業端點偵測與回應模組的攻擊鏈視覺化功能，讓組織有信心針對整個環境中的特定 IOC (入侵指標) 與 MITRE 型 TTP (策略、技巧與程序) 搜尋過往威脅。

符合法令規範

為符合法令規範，組織可能需要保留更長一段時間的事件資料，以遵守資料保留與稽核的規定。只要運用 VMware Data Retention for VMware Carbon Black Cloud，您就能做好準備，可接受包括 HIPAA、NIST、PCI DSS 在內等組織的稽核。

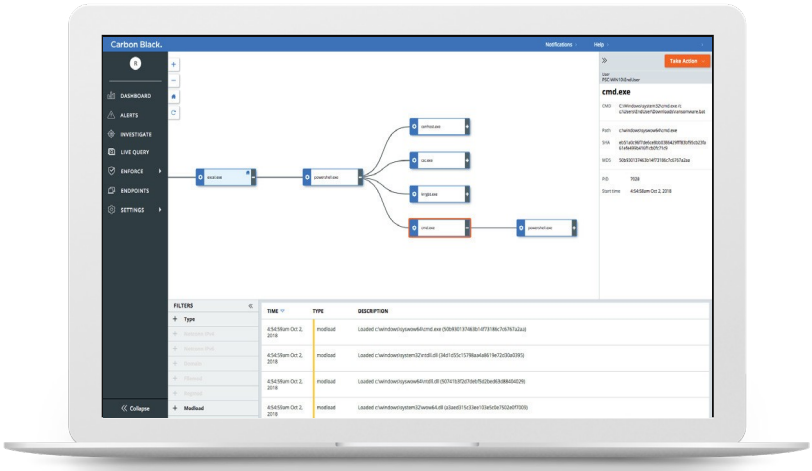


圖 1：企業端點偵測與回應會運用持續收集的端點活動資料，將廣泛的攻擊鏈視覺化，讓使用者清楚瞭解攻擊的每個階段究竟發生了什麼事。

vmware Carbon Black

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com 11073 台北市信義區松仁路 100 號 台北南山廣場辦公大樓 38 樓之一 電話 +886-2-3725-7000 傳真 +886-2-3725-7010 vmware.com/tw