VMware Carbon Black Cloud Managed Detection and Response

使用情境

- 支援安全性警示處理
- 為您的環境提供額外保護
- 讓安全性專家輔助您的團隊
- 安全性事件支援

優勢

- 推動更有效率且主動的安全性作業
- 提供可行性更高的警示，以防警示疲勞
- 透過通知為分析師提供寶貴的威脅情報，以及消除威脅所需的原則變更
- 縮短調查根本原因的時間
- 透過 24 小時全年無休的支援來減輕人員配置壓力
- 分析師可透過每月報告洞悉環境中的威脅並通知管理團隊
- 透過更清楚的檢視來掌握安全性趨勢，以協助引導原則
- 在安全事件應變期間，與安全性分析師互動溝通
- 威脅隔離

技能純熟的安全性專業人員短缺，是企業正面臨的問題；資安團隊經常花費過多時間監控與驗證警示，而無暇顧及其他安全需求。更令人擔憂的是，一旦發生攻擊，許多安全性分析師只能透過有限的工具與資料來分析所屬環境。他們也缺乏事件歷史的能見度與情境，導致情況更是雪上加霜。

VMware Carbon Black Cloud Managed Detection and Response™ 可提供關於攻擊的關鍵洞察，並針對修復威脅所需的原則變更給予建議。代管偵測與回應分析師會透過電子郵件通知您有威脅，並提供可在 VMware Carbon Black Cloud™ 中應對威脅的具體原則變更。此外，分析師也能提供您修復事件的指引，以及在事件發生時進行威脅隔離。

Carbon Black Cloud Managed Detection and Response 直接建置於 VMware Carbon Black Cloud 平台之上，由世界級的安全性專家團隊支援，他們會使用先進的機器學習 (ML) 與演算法工具集來監控及分析 VMware Carbon Black Cloud 中的資料。

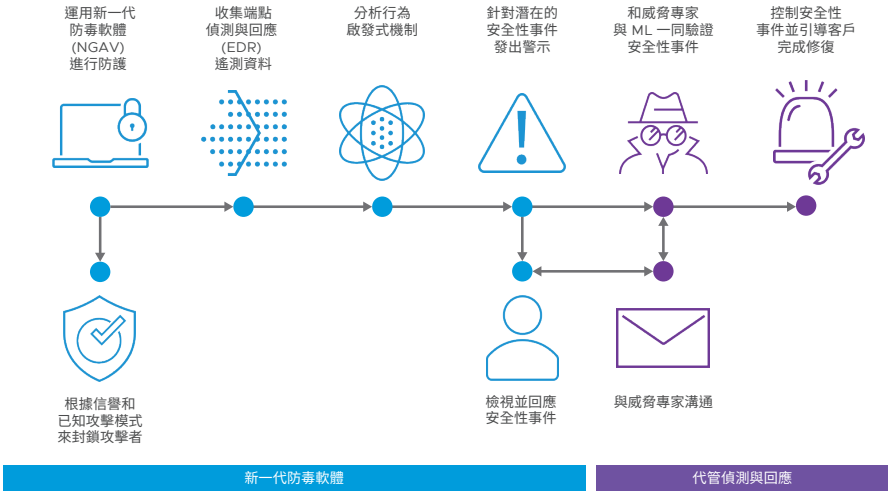

圖 1：Carbon Black Cloud Managed Detection and Response 作業流程。

「這是 VMware Carbon Black 的另一項出色服務。我立刻按照 Carbon Black Cloud Managed Detection 的建議採取行動，馬上就奏效了。[他們是]非常優秀的團隊。」

Integra Technologies 公司
IT 管理員
Chuck Baldwin

代管偵測與回應和 VMware Carbon Black Cloud

- 真人分析師使用 VMware Carbon Black Cloud 的未篩選資料來搜尋規避式威脅
- 全球威脅情報可協助我們在您實際受害前掌握攻擊趨勢
- 每月報告會針對您的環境提供額外的洞悉

功能

- 威脅驗證
- 電子郵件警示
- 根本原因分析
- 威脅諮詢
- 每月報告
- 與分析師進行安全事件應變的溝通
- 威脅隔離

使用 VMware Carbon Black Cloud 保護端點

透過可根據您需求調整的智慧型保護機制，實現端點安全性轉型。我們的雲原生保護平台可透過易於使用的單一主控台，結合必要的智慧型系統強化和行為防範功能，以阻絕新興威脅。VMware Carbon Black Cloud 藉由每天分析超過 1 兆筆安全性事件，主動找出攻擊者的行為模式，讓防禦者有能力偵測並阻止新興攻擊。

當今大多數網路攻擊都包含橫向移動、跳島和破壞式攻擊等策略，而在暗網上兜售的先進駭客技術與服務讓這個問題更加複雜。對於使用非集中化系統來保護高價值資產 (包括金錢、智慧財產和國家機密) 的目標對象而言，這些情況造成了極大的風險。

傳統的防禦方式使企業組織暴露於風險之中。網路宵小持續更新策略，並利用常見的工具和流程來掩飾他們的行動。您需要端點保護平台來協助您找出隱藏在細微波動下的惡意攻擊，並據此調整防護措施。

其他安全性產品只能收集與已知惡意行為相關的資料集，而我們則會持續收集活動資料，因為攻擊者會刻意佯裝正常行為來隱藏其攻擊行動。我們會分析攻擊者的行為模式，以偵測並防堵新型態攻擊。

使用 VMware Carbon Black Cloud 保護工作負載

隨著企業組織持續進行雲端轉型與應用程式現代化改造，他們需要功能強大又容易操作的現代化安全性解決方案。VMware Carbon Black Cloud Workload™ 所提供的進階保護功能，是專門為保障現代化工作負載所設計，能降低攻擊範圍，並強化安全態勢。

這項創新的解決方案結合了排定優先順序的弱點報告功能與基本工作負載強化，搭配領先業界的防禦、偵測與回應能力，針對在虛擬化、私有雲與混合雲環境中執行的工作負載提供保護。透過專為現代化資料中心所設計的工作負載保護，減少您的攻擊範圍並保障關鍵資產的安全。

Carbon Black Cloud Workload 與 VMware vSphere® 緊密整合，運用 VMware Tools™ 提供順暢的生命週期管理經驗。這麼做可減少安裝與管理費用，並整合多個工作負載安全性使用情境的遙測資料收集。透過這個統一解決方案，資安與基礎架構團隊得以自動保護安全性生命週期中每一點的全新與現有工作負載，不但簡化作業，還能與 IT 和安全性堆疊整合。

藉由專為當今需求打造的工作負載保護，取代多個安全性工具和代理程式，以及簡化跨 IT 與資安團隊的作業。運用 VMware 先進的工作負載保護，您可以封鎖已知與未知的進階攻擊，包括惡意軟體、無檔案和離地攻擊，同時提供單一資料來源以實現協同作業、減少阻礙並加速安全事件應變。

主要功能

威脅驗證與洞悉

提供 24 小時全年無休的服務，可透過滴水不漏的防護，讓您的團隊高枕無憂。VMware 的安全性專家會主動驗證警示，並傳送電子郵件通知，協助確保您的團隊不錯過重要警示。

從藍圖到根本原因

Carbon Black Cloud Managed Detection and Response 會為 VMware Carbon Black Cloud Endpoint™ Standard 及 Carbon Black Cloud Workload 警示提供額外的分析洞察 (例如由同一個根本原因造成的連線警示)，以協助您簡化調查，並解決安全性問題。

威脅爆發諮詢

VMware Threat Analysis Unit™ 會持續監控全球各地的威脅趨勢。如有大規模且值得注意的威脅爆發情況，我們的團隊將傳送包含入侵指標的諮詢內容給您，讓您的團隊能迅速評估風險並消弭落差。

每月報告

我們的代管偵測專家會提供每月報告，摘要說明您環境中的活動，包括最常見的可疑事件，以及最常成為攻擊目標的機器。這些報告是您調整原則的起點，能協助您的團隊綜觀趨勢並輕鬆回報問題。

與分析師進行安全事件應變的溝通

安全性事件發生時，您不必獨自面對。我們的安全性分析師 24 小時全年無休，可透過電子郵件進行雙向溝通，引導客戶的資安和 IT 團隊完成事件修復。

威脅隔離

我們的分析師使用 VMware Carbon Black Cloud 提供的強大工具，藉由更新雜湊信譽、調整行為防範規則以及在網路上隔離裝置，迅速阻止威脅情況惡化。

若要取得更多資訊或購買 VMware 產品

請致電 +886-2-3725-7000、造訪 vvmware.com/tw/products 或線上搜尋授權經銷商。如需詳細的產品規格和系統需求，請參閱 VMware Carbon Black Cloud Managed Detection 說明文件。

開始使用

VMware Carbon Black Cloud Managed Detection and Response 可提供給任何目前擁有 Carbon Black Cloud Endpoint 或 Carbon Black Cloud Workload 的客戶。

相關產品

如需有關 VMware Carbon Black Cloud 的詳細資訊，請造訪 vmware.com/tw/products/carbon-black-cloud。

如需有關 VMware Carbon Black Cloud Endpoint 的詳細資訊，請造訪 vmware.com/tw/products/carbon-black-cloud-endpoint。

如需有關 VMware Carbon Black Cloud Workload 的詳細資訊，請造訪 vmware.com/tw/products/carbon-black-cloud-workload。