

VMware Carbon Black Cloud Vulnerability Management

依照風險優先順序，針對端點與工作負載進行弱點評估

概觀

讓安全性團隊能在 Carbon Black Cloud 主控台內，直接依照風險優先順序，無需透過掃描即可查看弱點和情境，進而主動降低風險。

優勢

- 依據風險和攻擊潛勢排定弱點評估的優先順序
- 運用 Kenna Security 的資料科學方法的內建風險評分
- 減少時間點掃描對效能的影響
- 著重於對端點和工作負載構成真正風險的弱點，以減少誤報和干擾警示
- 運用開放式 API 進行整合，並將修復工作流程自動化

解決方案平台

- Windows：Windows 7、10
- 伺服器：Windows 2008 R2、Windows 2012、Windows 2012 R2、Windows 2016、Windows 2019
- Linux：RHEL 8、CentOS 8、Oracle 8、SUSE、Ubuntu、Amazon Linux、Debian

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.com/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

安全性與 IT 團隊正面臨弱點數量倍增又亟待解決的頭疼問題。團隊在缺乏情境和能見度的情況下，無法了解弱點對其資產所構成的風險，因此，他們難以協調修補程式部署和修正措施的優先順序，而為組織的整體安全態勢帶來不必要的風險。

識別風險以強化端點和工作負載

Carbon Black Cloud Vulnerability Management 運用 Kenna Security 經實證的資料科學方法進行弱點風險評分，讓安全性團隊能專注於修補或修復其環境中最關鍵的弱點。

Carbon Black Cloud Vulnerability Management 可讓團隊直接存取弱點情報和情境，以確保優先修復構成最高安全性風險的弱點，然後再修復次要弱點。依照風險優先順序處理的方法著重於弱點的已知攻擊潛勢和行為，運用此方法可減少需要解決的弱點數量，而且不會對端點和工作負載造成不必要的風險。

Carbon Black Cloud Vulnerability Management 在端點和工作負載上運用現有的輕量型代理程式，將監視清單資料提供給 Kenna Security 進行評估。分析師能直接在 Carbon Black Cloud 主控台內即時掌握端點和工作負載上的弱點，免除手動掃描的額外負荷。



圖 1：VMware Carbon Black Cloud Vulnerability Management 之弱點概觀

Kenna Security 的風險評分

Carbon Black Cloud 與 Kenna Security 攜手合作，提供容易理解的弱點風險評分。Kenna Security 的風險型弱點管理方法結合了資料科學、機器學習和預測性模型，以減少手動排列優先順序和風險評分的流程，讓團隊能專注於主動降低整體風險。

風險分數考量多項因素，包括已知的攻擊與影響、威脅情報摘要、傳統弱點評分指標 (CVSS) 以及軟體監視清單，以真實呈現真正與弱點相關的風險。只要將所有這些因素納入考量，安全性團隊就能掌握其環境中最關鍵的弱點清單並加以解決。

