

VMware Carbon Black Container

常見問題

功能與支援

問：VMware Carbon Black Container 的主要功能是什麼？

答：主要功能如下方所列：

- 容器映像掃描
 - 為生產環境中正在執行的所有容器提供能見度，並確保已對其進行掃描以落實安全性原則。限制生產環境中允許的倉管中心和存放庫，按嚴重程度排定弱點的先後順序，並確保僅將已核准的映像部署到生產環境。
- 安全態勢儀錶板
 - 提供單一介面，讓您完整取得跨 K8s 叢集和命名空間的安全態勢能見度，包括違反規則和設定的能見度。查看弱點和設定錯誤的整合風險評分。
- 排定風險評估優先順序
 - 透過掃描持續整合 (持續整合 / 持續交付) 和在 Kubernetes 叢集上的 Kubernetes 資訊清單，以及在部署容器之前偵測和預防弱點的功能，優先處理 Kubernetes 環境中最嚴重的風險。
- 持續整合 / 持續交付管道整合
 - 整合至開發人員生命週期中，以便在應用程式部署到生產環境前，能先分析並控制應用程式風險。在建置 / 部署生命週期的早期掃描容器和 Kubernetes 設定檔，就可加快解決弱點和設定錯誤的狀況。將開發安全營運自動化，為 Kubernetes 工作負載的完整生命週期持續提供雲原生安全性與合規。
- 治理與強制執行
 - 透過控制部署至叢集的工作負載並提供能見度，確保 Kubernetes 設定的完整性。自訂的原則會透過封鎖或警示異常來強制執行安全設定。
- 合規性原則自動化
 - 左移至開發週期，可在建置時偵測和預防弱點。建立自動化原則以強制執行安全設定並確保符合組織需求及業界標準，例如 CIS 基準測試。
- 自訂查詢
 - 針對工作負載安全態勢與治理取得深入的能見度以確保合規，並能透過自訂查詢自由探索 Kubernetes 工作負載設定。
- 網路連線對應
 - 瞭解應用程式架構、不同工作負載之間的連線，以及工作負載如何透過來自叢集外之外部來源的流出連線來使用服務。
- 執行階段映像叢集掃描
 - 掃描弱點，以確保正在執行的任何工作負載中所使用的容器映像都是最新狀態，並偵測弱點。
- 整合式警示儀錶板
 - 將事件與警示整合到單一儀錶板，以便加快調查和連結來自主機及容器層的事件。
- Kubernetes 能見度對應
 - 透過風險評分取得工作負載弱點、設定錯誤和違反原則情況的能見度，進而更妥善地降低風險
- 異常偵測
 - 瞭解正常網路行為的樣貌，並透過警示識別惡意網路活動。
- 流出和流入安全性
 - 保護到私有和公有目的地的流出連線。找出具有 IP 信譽的惡意流出連線。
- 威脅偵測
 - 掃描開放式連接埠是否有弱點，以快速偵測和發現橫向攻擊和進行中的攻擊

問：Carbon Black Container 只適合 Kubernetes (K8s) 環境嗎？

答：無論使用何種協調作業系統，Carbon Black 容器安全性都可以掃描映像來查找弱點。映像掃描工具 (cbctl) 的設計是為了與持續整合 / 持續交付管道整合，以協助支援此領域解決方案所預期的左移安全性。

Kubernetes 是我們目前唯一支援的容器協調作業平台。Carbon Black Cloud 將為各種工作負載類型提供安全性，包括虛擬化系統 (vSphere)、容器 (K8s) 和傳統伺服器系統。我們的容器安全性產品特別加入了跨地端、私有雲和公有雲環境保護 Kubernetes 工作負載的支援。

問：各個套件中提供了哪些功能？

答：Container Essentials 套件包含下列功能：

- 容器映像掃描
- 安全態勢儀錶板
- 合規性原則自動化
- 排定風險評估優先順序
- 治理控制與強制執行
- 持續整合 / 持續交付的整合
- 拓撲圖
- 叢集映像掃描

Container Advanced 套件包含 Container Essentials 的所有項目，以及下列功能：

- 整合式警示
- 威脅偵測
- 流入與流出安全性
- 工作負載異常偵測

問：哪些廠商 / 技術在公有雲和私有雲中受到支援？

答：我們的解決方案支援 Kubernetes (雲端或地端的開放原始碼版本)、PKS/Tanzu、GKE (Google K8s 引擎)、Open-Shift (RedHat)、AKS (Azure K8s 服務)、Amazon EKS。

安裝

問：安裝的先決條件是什麼？

答：安裝之前必須滿足以下條件：

1. Kubernetes 安全性開發營運 (DevOps) 或超級管理員角色已在 Carbon Black Cloud 主控台上指派給您。
2. Kubernetes 叢集的管理員權限
3. Kubernetes 叢集具備已啟用 ValidatingAdmissionWebhook 的許可控制外掛程式。
4. 可使用 Kubernetes 指令行工具 kubectl 控制 Kubernetes 叢集。
5. Kubernetes 叢集節點可以針對連接埠 443 上的 https 要求存取 CBC 環境的 URL。該 URL 是您正在使用的 CBC 環境。
6. Kubernetes 叢集節點可以針對連接埠 443 上的 gRPC 流量存取事件串流 URL。
7. Kubernetes 叢集節點可以從 Docker Hub 倉管中心提取容器映像。

資源

問：我可以在哪裡找到容器安全性產品的技術說明文件與示範？

答：技術說明文件可在 TechZone 找到：

- [TechZone – Carbon Black 容器路徑](#)

問：我可以在哪裡找到更新版發行注意事項？

答：可使用此連結找到更新版發行注意事項：[發行注意事項](#)

問：我可以到哪裡取得其他資源並深入瞭解容器？

答：如需 VMware Carbon Black Container 的詳細資訊，請參閱 [TechZone 中的 Container 常見問題頁面](#)。如要深入瞭解容器、Kubernetes 和雲原生應用程式，我們建議造訪 [KubeAcademy](#)。

