Trend Vision One™ – Container Security

採用進階映像掃描、政策導向核准控管，以及執行時期防護、偵測及回應來簡化容器防護

現代化應用程式開發策略在一些希望加速推出和供應最新功能的企業之間，越來越普及，並且為客戶創造出更多的價值。儘管雲端原生應用程式開發擁有說不完的好處，但卻伴隨著一項重大風險，那就是缺乏資安防護以及資安工具不連貫。今日企業面臨著必須同時達成資安團隊與應用程式團隊目標的挑戰，因為兩者不論在資源和優先次序上都不盡相同。除此之外，微服務架構也正在改變企業移轉至雲端、容器與無伺服器平台的方式，所以需要一套整合式平台來提供雲端防護。

由於技術上的諸多優點，容器已逐漸蔚為主流。根據雲端原生運算基金會 (Cloud Native Computing Foundation，簡稱 CNCF) 指出，**88%** 的企業都在使用容器，而且大部分都是用在營運環境。此外，容器環境也變得多樣化，許多企業都在企業內或雲端上執行容器，而 Kubernetes 也成為容器協調與作業簡化的標準輔助工具。

資安團隊正面臨新的挑戰

隨著企業將營運工作負載移轉至雲端原生平台，再加上 DevOps 將資安實務原則全面套用到建構流程與執行時期部署環境，資安解決方案的設計必須要能成功橫跨混合雲與多重環境 (實體、虛擬、雲端、容器及無伺服器)。隨著資安團隊承擔了更多的雲端防護責任，您需要從建構時期到執行時期都建置值得信賴的控管。如此才能促進工具的整合以及資安與法規遵循要求的彼此配合，卻不干擾持續整合/持續交付 (CI/CD) 的開發循環。

向您介紹 Trend Vision One™ – Container Security

提供容器映像防護、容器核准控管政策，以及容器執行時期防護、偵測及回應。Container Security 可更早、更快偵測惡意程式、漏洞，以及法規遵循問題。您的資安營運與應用程式團隊都能在營運環境的漏洞遭到攻擊之前預先加以解決和矯正，以降低成本與複雜性。

定義一次性政策並管理容器風險

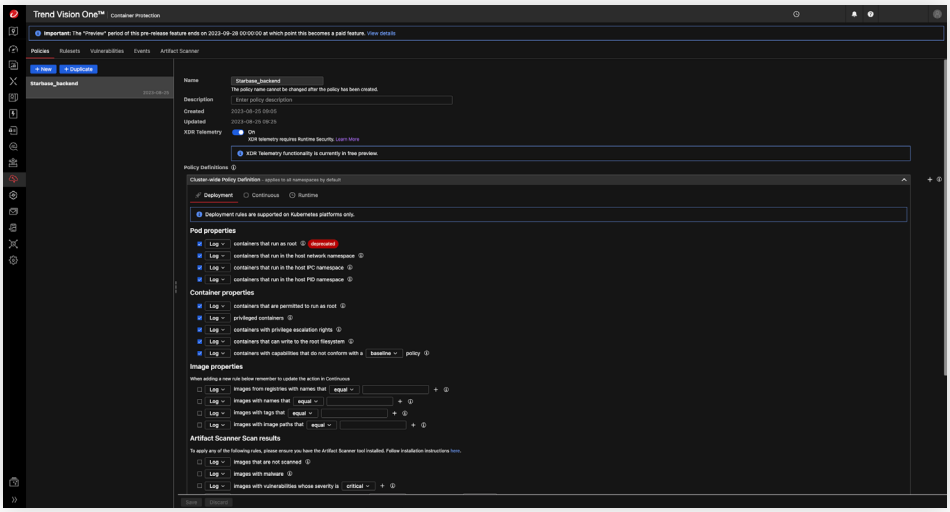
透過容器核准控管來選擇及定義政策，唯有最安全的 Kubernetes 容器才能夠部署。與 Kubernetes 直接整合的 Container Security 可定義允許或禁止映像執行的政策，根據您定義的一次性偏好設定來加以控管，包括：是否為特權容器，或者是否已經掃描過惡意程式和漏洞，這樣一來，您的資安團隊就能掌控您環境內所能執行的容器。

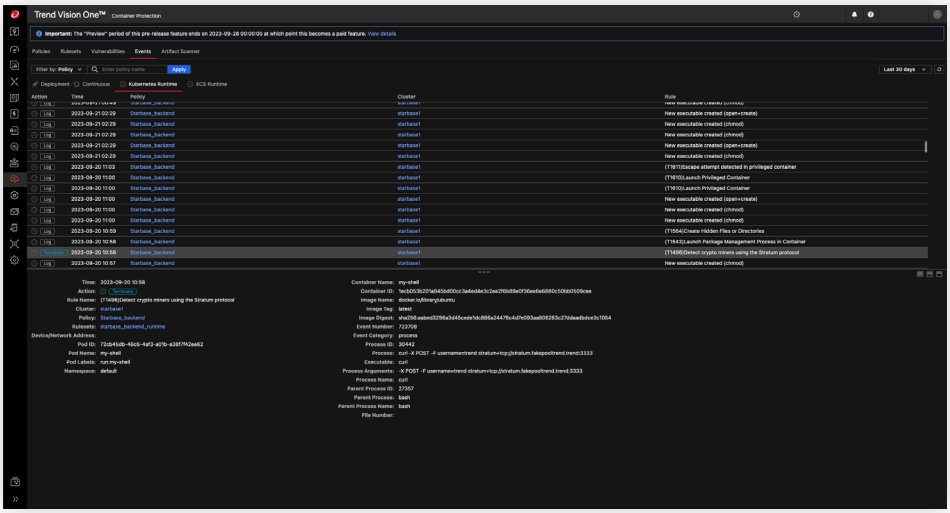
執行時期防護能為您的資安團隊帶來一道額外的防禦，提供涵蓋所有執行中容器應用程式的警報與攻擊指標 (IoA)，以及對應 MITRE ATT&CK 框架的洞見。取得執行中容器的風險可視性，發掘試圖執行不允許指令或非法存取檔案的情況，並透過延伸式偵測及回應 (XDR) 功能來偵測和回應可疑活動。

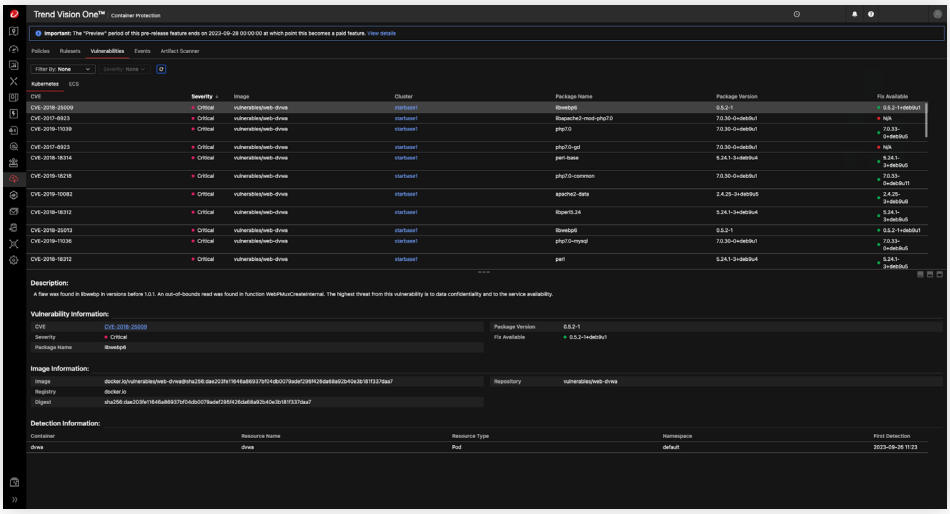
端對端容器防護

Container Security 可協助 DevOps 團隊從建構流程到執行時期一路部署立即而持續的防護。Container Security 支援目前主流的容器平台，包括：Amazon EKS、Amazon ECS、AWS Fargate、Azure AKE 以及 Google GKE，能與您現有的各種 CI/CD 工具流程及容器環境無縫整合。提早在軟體建構流程前期導入有效的資安防護，讓開發流程更快取得穩定的成果，同時減少手動資安步驟與應用程式停機時間。不僅如此，執行時期防護、偵測及回應還能保護執行中的容器，防範不斷演進的威脅，跨防護層調查威脅活動。透過清晰、條理分明的 Kubernetes 叢集盤點來簡化資源管理。

核准控管政策







第三方認證的領先地位

- Forrester New Wave™ 領導者: 延伸式偵測及回應 (XDR) (2021 年第 4 季)
- 雲端工作負載防護市場占有率 (Cloud Workload Security Market Share) 連續 6 年蟬聯第一 (2023 年)
- MITRE Engenuity ATT&CK (2023 年) - 防護力第一，能 100% 偵測所有評測中的關鍵攻擊步驟

主要優勢

在營運環境資安漏洞遭駭客攻擊之前預先加以解決

Container Security 能藉由映像掃描來偵測直接安裝的應用程式以及經由封裝管理員安裝的應用程式當中的威脅。透過可採取行動的洞見來快速修正問題，讓開發人員利用現有的工具和工作流程，在部署之前預先矯正問題。

持續確保容器安全

原生整合的政策導向部署控管，確保您營運環境中所執行的 Kubernetes 部署環境皆安全無虞。

Container Security 可讓您建立政策來允許或攔截部署動作，根據 Pod 與容器的防護要求以及映像與登錄掃描的結果來訂定規則。當映像準備經由 Kubernetes 部署時，就會觸發負責核准控管的 Webhook 來檢查該影像是否安全可以放行，從而允許或防止映像執行。

具備完整可視性、偵測及回應的防護

一旦完成部署，就能為容器提供執行時期防護，進而多一分保障。利用 XDR 來發掘及攔截可疑活動，掌握含有漏洞的執行中容器以及容器偏離的情況，偵測、追蹤和調查跨防護層的威脅或活動。

要進一步了解主機式防護，請前往 Trend Vision One™ – Workload Security 網頁。

Container Security 功能

1. 持續的自動化容器映像掃描

掃描什麼：

Container Security 可掃描容器映像來產生一份軟體物料清單 (SBOM)，讓您確保所有問題都能及早修正，並且交叉核對映像中的套件與其修補版本以減少誤判的情況。Container Security 的映像掃描可達成以下目的：

- **惡意程式偵測。**
- **漏洞評估。**
- **政策遵循。**

掃描您 CI/CD 建構流程中的映像，確保您的容器映像從一開始就安全無虞，並且持續防範未來的不明威脅。

2.容器核准控管政策

Container Security 採用原生方式與 Kubernetes 整合，可定義政策來確保唯有符合規定的容器能在營運環境中執行。Container Security 的核准控管政策可讓您：

- **根據容器映像掃描及偵測結果來建立政策。**
- **唯有符合特定應用程式或企業資安政策的映像可以在 Kubernetes 內執行。**
- **定義進階政策 (例如禁止映像設定為特權容器) 或者根據名稱或標籤來允許例外情況。**

3.容器執行時期防護

執行時期防護可確保您環境內執行的容器持續受到防護，即使已經完成部署動作，您可以：

- **盤點 Kubernetes 叢集。**
- **掌握含有漏洞的執行中容器。**
- **防止試圖執行不允許指令、非法存取檔案、容器偏離等情況，以及其他惡意活動。**
- **利用延伸式偵測及回應 (XDR) 提供的情境來偵測、追蹤、調查橫跨防護層的威脅或活動。**

系統需求

- Kubernetes® 1.14.0 或更新版本，以及通過 Certified Kubernetes 認證的平台。
- Helm 3.0.1 或更新版本。

如需更多資訊，請至：trendmicro.com/container_security

部署與整合

Container Security 可當成您 CI/CD 流程當中的一個重要步驟。

要執行政策導向的部署控管，請先建立一個 Kubernetes 叢集 (或者開啟您現有的 Kubernetes 叢集) 然後再安裝政策導向部署控管元件。接著，建立一個政策來讓 Container Security 套用到整個叢集。最後，測試這個政策是否運作良好。

請參閱 Trend Vision One – Container Security Documentation 網頁來取得有關如何開始使用以及應用案例等更多資訊。

如需更多資訊，請至：trendmicro.com

©2023 年版權所有。趨勢科技股份有限公司及其相關機構保留所有權利。Trend Micro、ｔ字球形標誌、Apex One 及 Trend Micro Apex Central 是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為該公司的商標或註冊商標。本文件之內容若有變動，恕不另行通知。[DS05_Vision_One_Container_Datasheet_231011TW]

如需有關我們蒐集哪些個人資訊的詳細內容和理由，請參閱我們網站上的「隱私權聲明」：trendmicro.com/privacy