

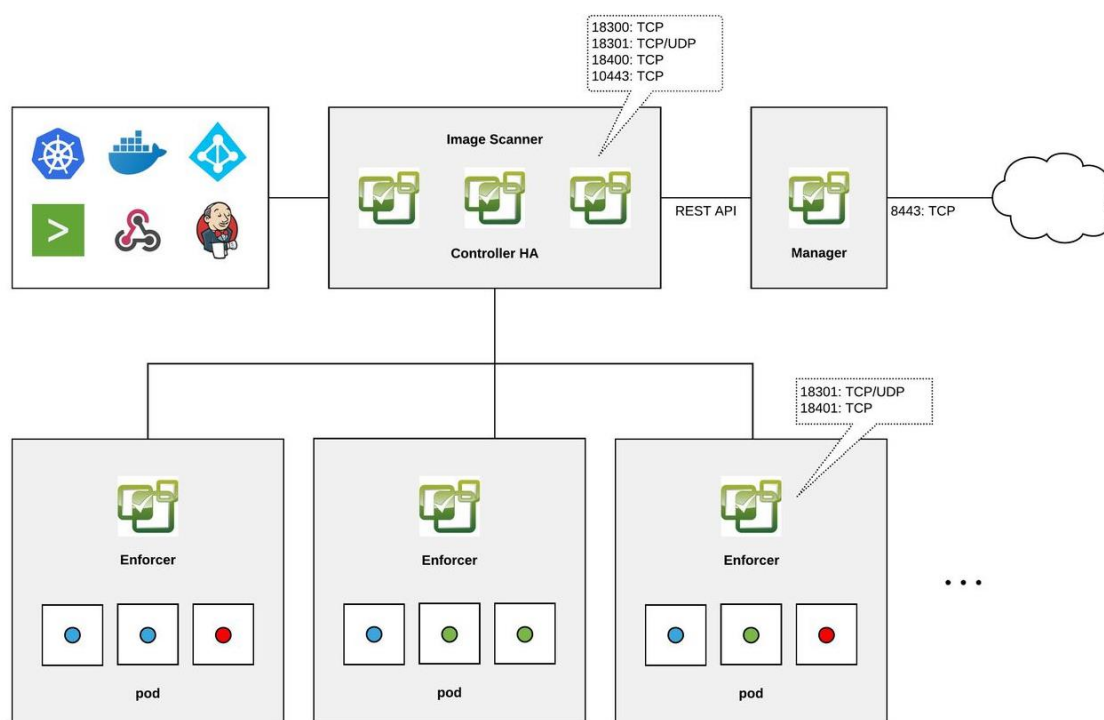
Suse NeuVector

Kubernetes 安全防護員



Kubernetes 已逐漸成為企業 IT 的應用系統架構之一，Kubernetes 的核心技術是容器虛擬化技術與獨立的虛擬網路，對於 IT 的資訊安全管理而言，面對現今層差不窮的網路攻擊行為，資訊安全無法單純只靠傳統的資訊安全防護機制來管理 Kubernetes 平台，無法滿足 IT 的資訊安全規定，需要一套專門針對 Kubernetes 平台設計且獨立於傳統的資安防護管理的資安防護工具來管理與防護；**Suse NeuVector** 是一套針對 Kubernetes 環境的資安全防護平台，提供 Kubernetes 環境下 container 運作的即時圖形化儀表板呈現整個環境的安全漏洞與網路存取拓譜圖，並且主動隔離可能有問題的 container，並防護異常網路存取，提供企業 Kubernetes 上的應用系統一個穩定安全的運作環境。

NeuVector 架構



圖(一) NeuVector 架構

NeuVector 的架構由 Controller、Enforcer、Manager、Scanner 與 Updater 五個元件，五個元件各功能：

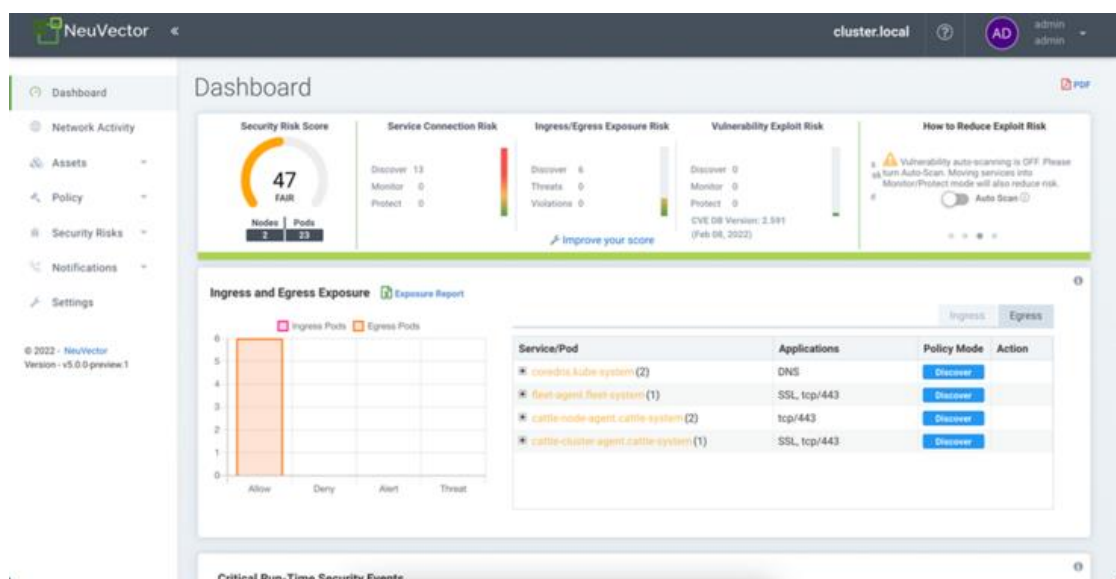
- Controller：NeuVector 的核心元件，透過 controller 來管理整個平台，並提供 API 介面，做整個環境管理；NeuVector 提供 HA 架構提供整個平台運作的穩定。
- Enforcer：主要提供安全性策略的佈署與執行，它的運作是以 DaemonSet 方式佈署，來提供整個 Kubernete 的安全防護。
- Manager：提供 Web-UI 的數位儀表板管理介面與 CLI 操作介面，並且提供使用者權限管理 NeuVector 的整個平台操作。

- Scanner：提供 Kubernetes、Container 與 Image 做安全性漏洞掃描，並提供各漏洞的詳細資訊供，以利漏洞修復的參考。
- Updater：用於 NeuVector 的 CVE 漏洞的更新。

NeuVector 主要功能

- 安全漏洞掃描

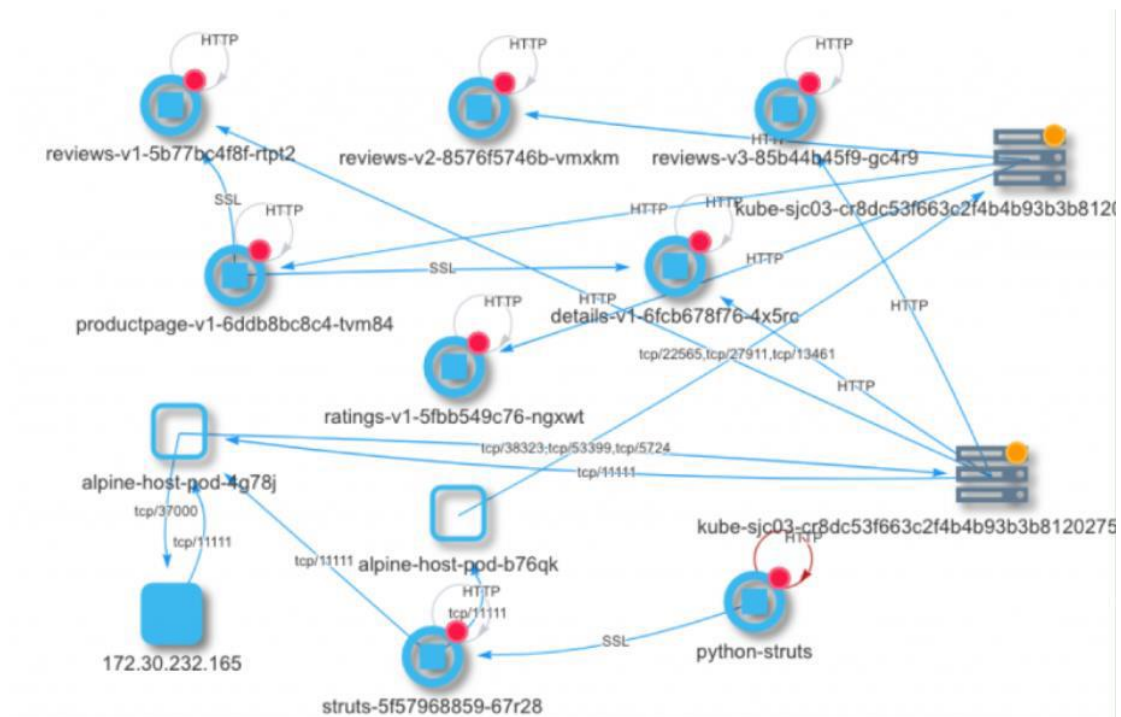
NeuVector 主動對 Kubernetes 環境的安全漏洞掃描，並且將目前環境的掃描出來的安全漏洞資訊即時呈現在數位儀表板上，提供詳細資訊供管理者參考，了解現行環境中有那些安全性漏洞問題，讓管理者能充份掌握整個 Kubernetes 的環境狀況。



圖(二) 數位儀表板

- 容器網路拓譜圖

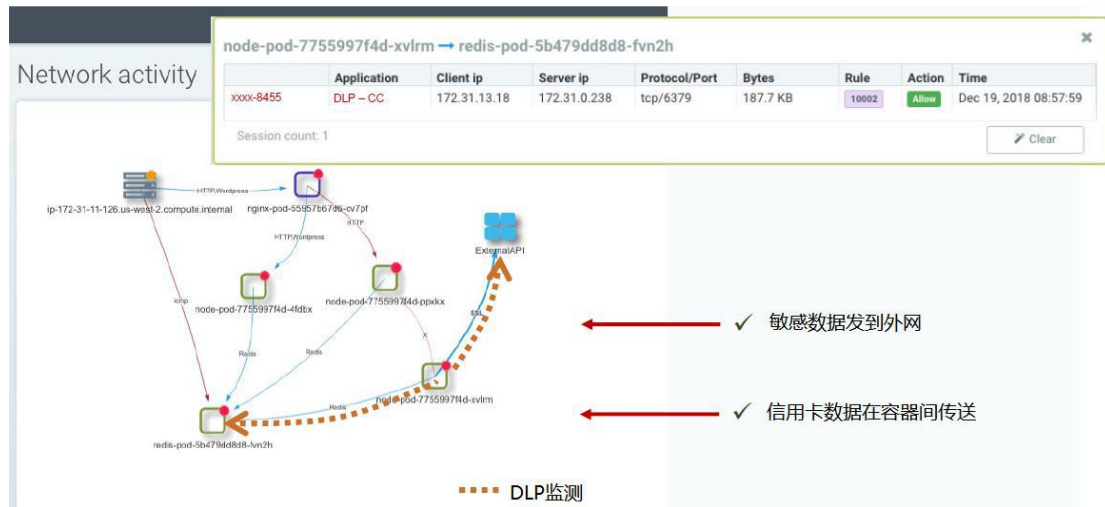
NeuVector 主動探測 Kubernetes 的網路活動，並且繪製出 Kubernetes 中的 container 運作時的網路存取行為，並且還可以將整個 Kubernetes 中整個網路運作活動用網路拓譜圖方式呈現，讓維運管理人員清楚掌握 Kubernetes 平台中的網路活動運作，如下圖(三)所示：



圖(三) 系統網路拓譜圖

- 網路政策定義

NeuVector 提供多組內建的安全防護規則與自定義防護政策防護機制，以防範 container 之間的異常網路存取，監測並且止敏感資料的異常傳遞，防範資料外洩的資安問題，如下圖(四)所示：



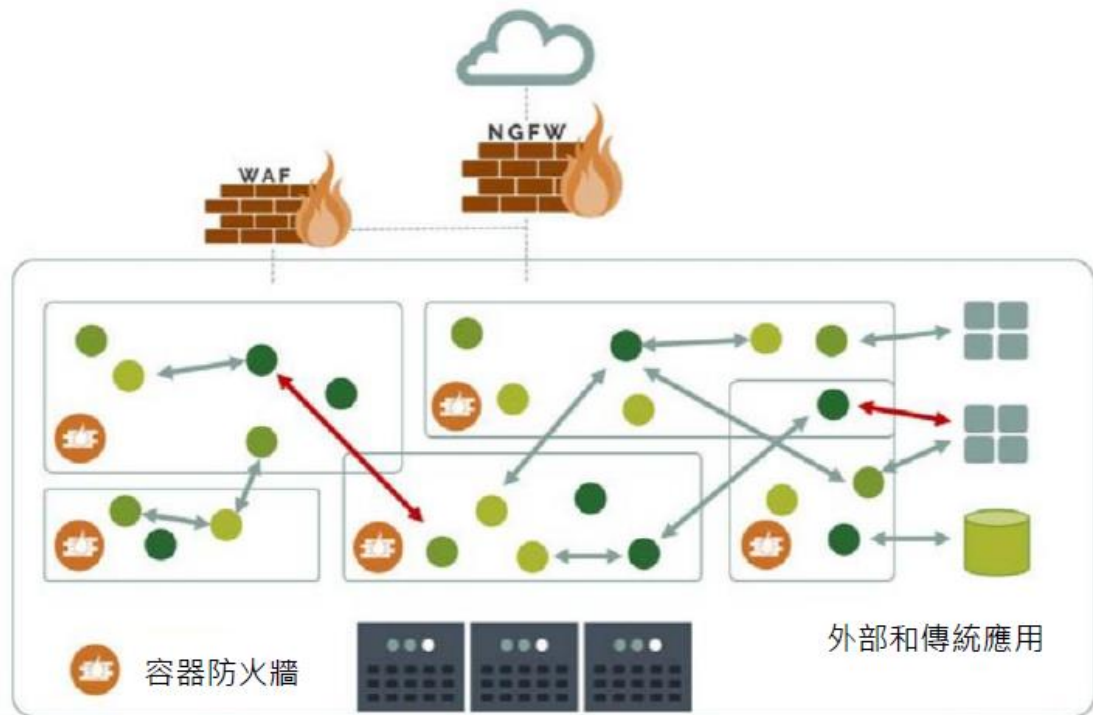
圖(四)白名單政策

● L7 防火牆

提供主動性容器防火牆為容器提供即時安全防護，提供下面防護機制：

- ✓ 主動聲明式防控策略
- ✓ 白名單、黑名單安全性原則
- ✓ 主動化預測行為意圖分析
- ✓ 深入網路分析(DPI)
- ✓ 威脅防護
- ✓ 支持應用級別協定
- ✓ 容器級別保護
- ✓ 與容器平台整合

提供上述多種防護機制保護容器平台運作的安全，如下圖(五)所示：



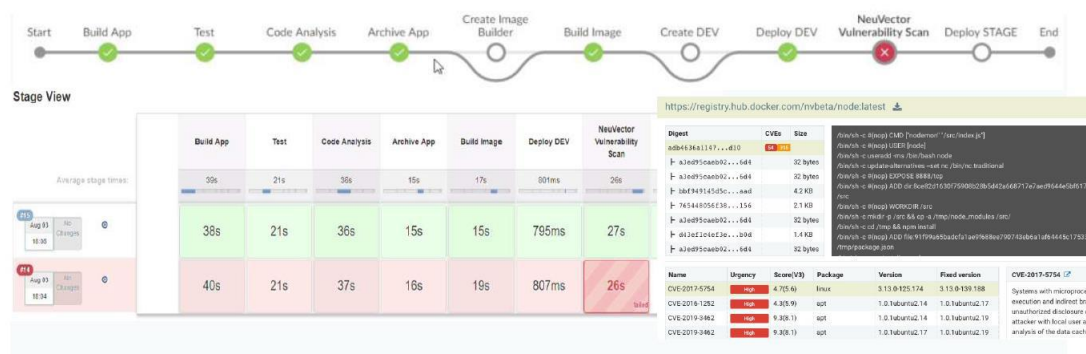
圖(五) 防火牆

- CI/CD 整合

NeuVector 能與企業的 DevOps 流程所使用 CI/CD 流程工具整合，提供下述幾項重安全管理的功能：

- ✓ 掃描公用、私有 Image Repository 掃描
- ✓ Image 漏洞分析
- ✓ 管理 Image 的發佈與佈署

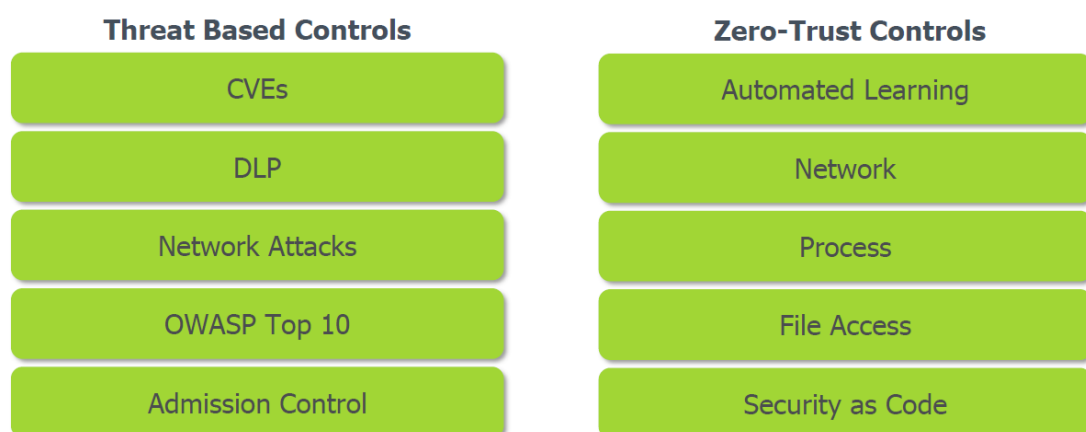
✓ 大量的 Image 的快速掃描



圖(六) CI/CD 整合

● 即時防護

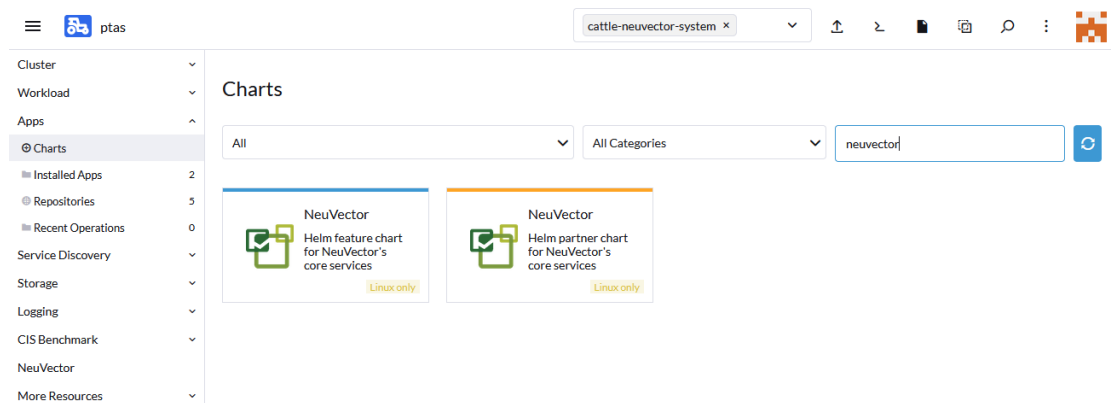
對於運行中的容器提供 Thread Based Controls 與 Zero-Trust Controls 防護，透過兩個不同的即時安全規則交互配合，提供完善的綜深防禦機制來保護 container 運作的安全。



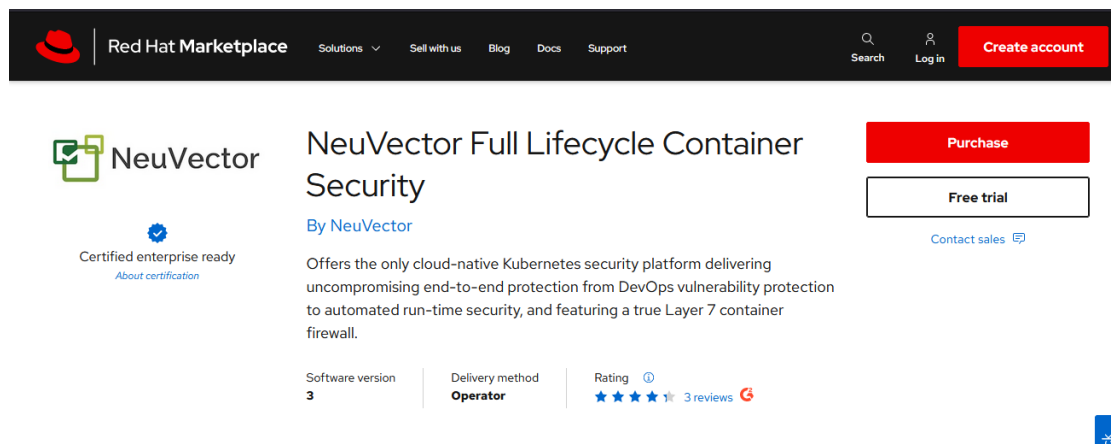
圖(七) 縱深防禦

- 快速佈署

NeuVector 的佈署建置相當簡單，它支援多種容器運作平台，同時它也認證成為多種容器運作平台的 Marketplace 上的應用程式，所以可以很容易透過容器平台的 Marketplace 來佈署 NeuVector 建置，如下圖(八)、圖(九)與圖(十)所示：



圖(八) Rancher Marketplace



圖(九) RedHat Marketplace



圖(十) Azure Marketplace

Suse NeuVector 是一套基於雲原生容器平台的安全防護解決方案，它可以透過各平台上的 Marketplace 來佈署 NeuVector 到 Kubernetes 的運作平台上，佈署完後即可以立即對所佈署環境提供即時的安全防護，以確保企業應用程式運作在一個安全環境下；此外亦可以檢測企業應用系統是否有安全漏洞，並提供完整安全性漏洞資訊供 IT 來做安全性漏洞排除，來補足企業對於 Kubernetes 安全性的不足。

有需要諮詢協助的地方，可直接聯絡：

架構服務處

處長 陳金生 Edward Chen

02-27316868 分機 820

edwardchen@mpinfo.com.tw