Trend Cloud One™ – Container Security

融入您 CI/CD 自動化流程的持續性容器映像與登錄防護

為了提升應用程式開發速度，建立連貫的應用程式生態系，雲端優先的應用程式開發策略在企業間日益普及。然而，今日企業卻覺得很難管理傳統資安解決方案來配合 DevOps 團隊及營業單位的要求，因為兩者所需的資源以及分配的優先次序並不相同。除此之外，微服務架構的應用程式開發方法，也開始改變企業移轉至雲端、容器及無伺服器平台的方式。

根據 IT 分析研究機構 ESG 的研究指出，自 2017 年開始，已致力或有興趣導入混合雲策略的企業已從 81% 成長至 93%。此外，根據 Gartner 的估計，隨著雲端優先的策略持續發展，到了 2026 年，全球超過 90% 的企業都將在營運環境當中執行容器化應用程式，較 2021 年的 40% 大幅成長。同時，Help Net Security 的研究也指出，60% 的受訪者表示 Kubernetes 是他們部署營運應用程式偏愛或唯一的方式，而且目前已經有 43% 的工作負載部署在 Kubernetes 上。

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)。想要打破 IT 資安與 DevOps 之間的藩籬，讓雙方發揮集體綜效，您需要一套值得信賴、一路涵蓋建構時期到執行時期的資安控管。如此可促進工具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。

Trend Cloud One™ – Container Security* 能提供容器映像與登錄防護、容器核准控管政策，以及容器執行時期防護。Container Security 的容器與登錄掃描是專為您的開發人員與資安營運團隊設計，能更早、更快偵測惡意程式、機密/金鑰、法規遵循問題以及漏洞，包括開放原始碼相依元件當中的漏洞。除此之外，我們的 Trend Cloud One 解決方案，能讓您利用趨勢科技領先業界的防護來偵測封裝管理員安裝的應用程式以及直接安裝的應用程式中的威脅。而 Container Security 也能讓開發人員將 Snyk 的開放原始碼漏洞偵測能力融入流程當中，提供開放原始碼相依元件漏洞的早期偵測與矯正。

藉由容器核准控管，唯有經過政策核准含有合法憑證的映像以及符合預先定義政策的映像才能被部署。經由與 Kubernetes 開放式政策代理程式直接整合，Container Security 可定義允許或禁止映像執行的政策，根據一些預先定義的條件來加以控管，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。

Container Security 執行時期防護可為您的 IT 團隊提供一道額外的防禦。這套雲端原生防護軟體服務 (SaaS) 解決方案提供您涵蓋容器化應用程式的警報與攻擊指標 (IoA)。當執行時期防護部署在叢集內以涵蓋每一節點內的容器化應用程式時，它會藉由「學習模式」來建立一套預期行為的模型。

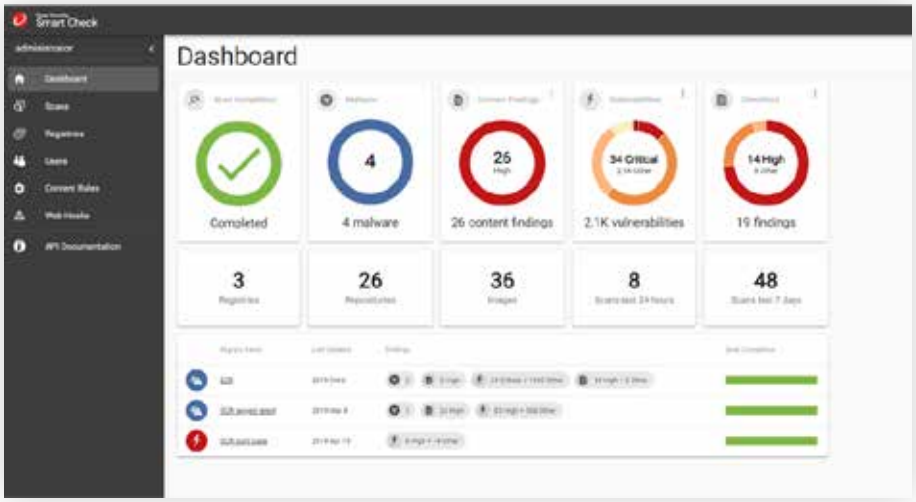
專為 DevOps 最佳化的端對端掃描

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 是專為 AKS、EKS 及 GKS 等主流容器平台而最佳化，可無縫整合至您現有的工具流程。您將獲得完整的自動化功能，經由特別開發的完整 API 與您現有的 CI/CD 流程整合。應用程式架構師與開發人員可透過程式碼將防護融入建構流程來執行容器與登錄掃描。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。

現代化雲端原生防護

我們遍布全球的 15 個研究中心與 450 名內部研究人員，再加上不干擾 CI/CD 流程的資安防護，您的 IT 團隊就能更早發現問題，減少開發時程及工作流程中斷的情況。Container Security 可讓您的資安工程師在不影響生產力的情況下達成法規遵循要求，利用客製化政策來執行政策遵循掃描。此外，您的資安團隊還可掌握執行時期的可視性，偵測嘗試執行被禁止的指令、或是存取無權存取的檔案等類似的行為。除了儀表板上的資訊之外，還有通知和詳細的歷史記錄檔可輕鬆產生報表和執行稽核檢查。

Container Security 容器映像與登錄防護



Container Security 核准控管政策

主要優勢

從建構時期到執行時期一路防範漏洞攻擊

有了趨勢科技領先業界的防護，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存在的威脅。獨家的 Snyk 開放原始碼漏洞資料庫，可提早偵測並解決開放原始碼相依元件的漏洞。

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。

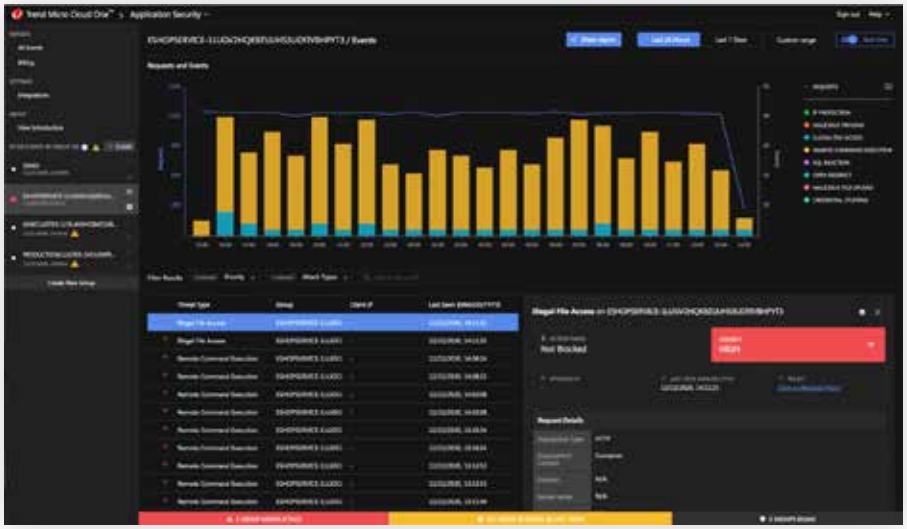
專為 DevOps 最佳化的防護

Container Security 讓您的應用程式架構師與開發人員透過程式碼將防護融入建構流程當中，提供容器映像與登錄掃描。提早在軟體建構流程前期導入有效的資安防護，讓您的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。

涵蓋完整生命週期的容器防護

除了 Container Security 之外，還有 Trend Cloud One™ - Workload Security 提供的主機防護來保護您的容器主機並且在作業系統層次進行整合。它能利用即時的惡意程式掃描來防範惡意檔案，並透過入侵防護服務來防止駭客從遠端攻擊軟體漏洞。此外，Workload Security 還能提供最佳的網路流量檢查，包括橫向與縱向的流量。Container Security 與 Workload Security 的搭配能確保您的容器環境獲得完整的防護。

Container Security 容器執行時期防護



Container Security 功能

1. 持續的自動化容器映像掃描

掃描什麼：

容器映像防護在掃描時會將映像層層解開，然後詳細掃描您的內容。這讓您確保所有問題都能及早修正，並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：

- 偵測惡意程式。
- 評估漏洞。
- 搜尋是否含有機密資料，如私密金鑰和密碼。
- 政策遵循。
- 經由 Snyk 掃描開放原始碼漏洞。

如何達成：

要達成持續的掃描有兩種建置方式，第一種是建置在 CI/CD 建構流程當中，在容器映像推送至登錄之前。第二種是持續不斷掃描容器登錄來偵測現有的映像是否含有新的惡意程式與漏洞。如此可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。Container Security 可支援多種雲端服務廠商，包括 ECR、ACR 及 GCR。此外，您還可以利用 Container Security API 在您的建構流程當中呼叫掃描，根據掃描結果作為映像檢查證明 (Image Assertion) 與容器映像簽署服務的判斷依據。

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。透過程式碼將管理作業與政策自動化，成為 CI/CD 流程的一環。

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：

- 部署在叢集內來保護每個節點中的容器化應用程式。
- 更明確掌握嘗試執行已禁止指令或嘗試非法存取檔案的動作。
- 先透過學習模式來建立預期行為模型，當您準備上線營運時再切換至全面攔截模式。

4.管理主控台與存取控管

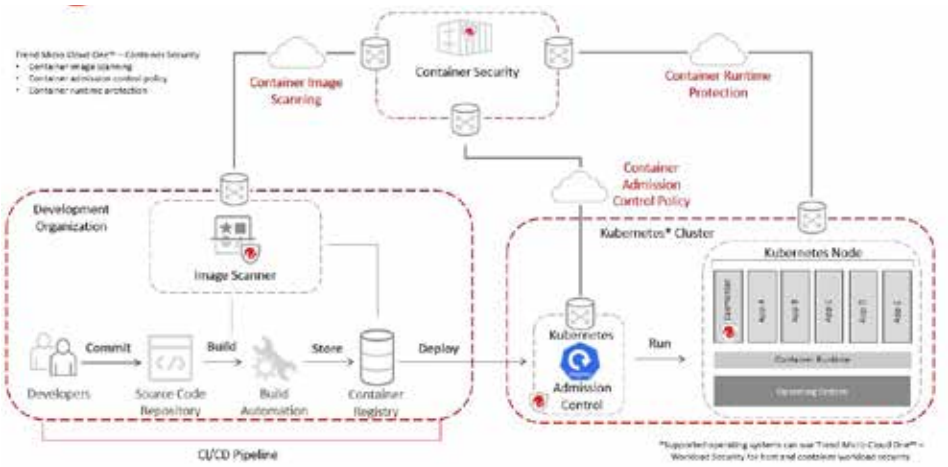
Container Security 提供一個豐富的圖形介面 (GUI) 管理主控台，內容包括：掃描涵蓋範圍儀表板、掃描結果、掃描目標 (檢視) 組態設定，以及角色導向存取控管 (RBAC) 的使用者與檢視管理。此圖形介面可提供下列資訊：

- 內容來源：已設定掃描/監控的登錄清單。
- 執行中掃描：任何正在執行的掃描狀態。
- 防護涵蓋範圍：目標登錄內有哪些映像已經掃描過了。
- 掃描警報：偵測到惡意程式、漏洞和機密的掃描結果。

世界級的威脅情報

隨時從趨勢科技及公開來源接收最新的威脅情報來提高掃描成效，讓您：

- 利用趨勢科技 Smart Protection Network™ 全球威脅情報 網來偵測惡意程式。
- 透過機器學習演算法來發掘零時差威脅。



Container Security 核准控管政策

安裝

Container Security 支援 Kubernetes 叢集架構。

- 公開下載點：https://github.com/deep-security/smartcheck-helm

Container Security 使用者可使用 Container Security GitHub 儲存庫 (Repository) 當中的指令列腳本 (shell script) 和 Kubernetes 資源。而該應用程式的映像，也可經由 Docker Hub 取得。

涵蓋容器完整生命週期的防護

Container Security 的映像掃描能與 Workflow Security 的進階執行時期防護相輔相成，讓容器獲得即時的惡意程式防護、容器漏洞防護、容器流量檢查，並且保護容器主機、Kubernetes 平台等等。

系統需求

- Kubernetes 1.14.0 或更新版本，以及通過 Certified Kubernetes 認證的平台。請參閱 www.cncf.io/certification/software-conformance/
- Helm/Tiller 2.14.1 或更新版本。
- 用來存取容器映像掃描系統管理主控台的 Google Chrome™ 瀏覽器。

可支援的登錄

Container Security 可允許列出目錄 (catalog) 並掃描任何支援 Docker V2 API 的登錄。

- Amazon Elastic Container Registry (ECR)
- Microsoft Azure Container Registry (ACR)
- Docker Trusted Registry (DTR)
- Google Container Registry (GCR)
- VMware Harbor
- JFrog Artifactory
- Sonatype Nexus
- Red Hat Quay Container Registry

如需更多資訊，請參閱：trendmicro.com/en_ca/ business/products/hybrid-cloud/cloud-one-container-image-security.html

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 Cloud 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。

建構安全、快速交付、隨處執行

支援以下平台：

Kubernetes 與 Docker：Container Security 能部署成一個 Helm Chart，因此很容易安裝到 Kubernetes 叢集內，提供進階的建構時期與登錄內映像掃描，偵測惡意程式、漏洞、機密與政策遵循狀況。此外，還有 Workflow Security 可在執行時期提供額外的容器防護，並且監控容器平台、協調工具、檔案與執行程序的變更，確保您容器的整個生命週期都受到妥善防護。

Amazon Web Services (AWS)：Container Security 能部署至 Amazon Elastic Container Service for Kubernetes (EKS) 來提供容器映像掃描，再配合 Workload Security 來提供額外的執行時期容器與 Amazon Machine Image (AMI) 工作負載防護，保護您的整個 AWS 環境。

Microsoft Azure：Container Security 可部署至 Azure Kubernetes Service (AKS) 來提供容器映像掃描，並透 Workload Security 來提供額外的執行時期容器與 Azure VM 防護。

Google Cloud™：您可將 Container Security 部署至 Google Kubernetes Engine (GKE) 來提供建構流程中的映像掃描，並透過 Workflow Security 來提供額外的執行時期容器與 VM 執行個體防護。將 Container Security 部署至 GKE 當中來提供跨多重雲端環境的掃描。

Red Hat OpenShift：Container Security 可部署至 OpenShift 環境內，為軟體建構流程提供進階掃描來保護您的應用程式。執行時期的容器則可搭配 Container Security (在可支援的主機上) 來加以保護，實現涵蓋完整生命週期的容器防護。

VMware Cloud™：Workload Security 具備與 VMware 各種服務整合的強大能力，確保您的虛擬及雲端工作負載 (包括容器在內) 皆獲得一致的防護，提供廣大的平台與核心支援、自動化政策管理，還有虛擬化監管程式 (Hypervisor) 層次的防護。

Container Security 是 Trend Cloud One™ 服務平台的一環，這套專為雲端開發人員設計的防護服務平台，還包括以下服務：

- Trend Micro™ Cloud Sentry：AWS 環境的威脅可視性，提供快速、可採取行動且符合您應用程式情境的洞見。
- Trend Cloud One™ – Conformity：雲端資安與法規遵循狀況管理。
- Trend Cloud One™ – Endpoint Security：涵蓋所有端點、伺服器及雲端工作負載的防護、偵測及回應。
- Trend Cloud One™ – File Storage Security：雲端檔案及物件儲存服務的防護。
- Trend Cloud One™ – Network Security：雲端網路層 IPS 防護。
- Trend Cloud One™ - Open Source Security by Snyk：開放原始碼漏洞與授權風險可視性與監控。
- Trend Cloud One™ – Workload Security：執行時期工作負載 (虛擬、實體、雲端及容器) 防護。

*趨勢科技的容器防護已將 Snyk 整合至 Trend Cloud One - Container Security 中 。

如需更多資訊，請至： trendmicro.com