Trend Cloud One™ – Workload Security

實體、虛擬、雲端及容器工作負載的執行時期防護

資料中心正在經歷一場巨大的蛻變，企業正紛紛將伺服器工作負載移轉至雲端，甚至導入容器和無伺服器等雲端原生應用程式架構。混合雲環境固然有諸多優點，但卻也帶來了新的風險和威脅。您的企業必須落實法規遵循，同時確保所有工作負載 (如：實體伺服器、虛擬、雲端以及容器) 都享有全方位的防護。

Trend Cloud One™ – Workload Security 在單一解決方案當中提供了專為伺服器、雲端及容器環境打造的全方位偵測及防護。Workload Security 不論面對何種工作負載都能提供一致的防護，同時更提供了一套豐富完整的應用程式開發介面 (API) 來讓您將防護自動化，避免干擾您的團隊運作。

自動化

資安程式碼 (Security as Code) 讓您的 DevOps 團隊將防護融入軟體建構流程當中，如此一來，您的軟體就能頻繁地推陳出新。經由內建的自動化，包括：自動搜尋與部署、快速啟動 (Quick Start) 範本，以及我們的 Automation Center，確保您的環境安全，迅速達成法規要求。

彈性

讓開發人員能自由選擇，廣泛支援各種平台的資安防護，能涵蓋混合雲、多重雲端、多重服務環境以及任何應用程式供應模式。

共存共榮

可採用 Trend Cloud One™ – Endpoint Security 服務來搭配 Workload Security，從單一解決方案保護使用者端點、伺服器以及雲端工作負載，並擁有統一的管理與角色導向存取控管。消除部署多套單一面向解決方案的成本與複雜性，並獲得專為您多樣化端點與工作負載而最佳化的特殊防護。

企業關鍵問題

✔ 自動化防護

透過涵蓋各種混合環境 (如資料中心和雲端) 的自動化防護政策、部署、運作狀況檢查以及合規報表，讓您在移轉或建立新的工作負載時能節省時間和資源。

✔ 完整防護

藉由單一代理程式來部署並整合實體、虛擬、多重雲端、容器以及使用者端點環境的資安偵測及防護。

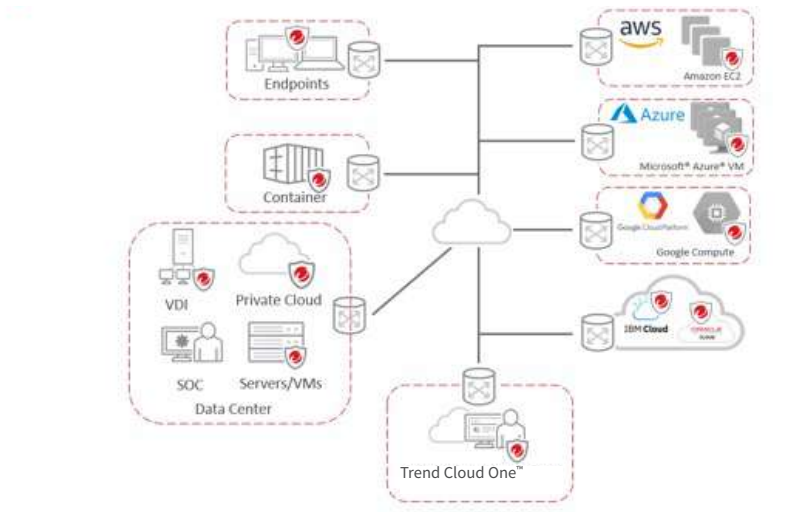
✔ 適合 CI/CD 流程的防護

提供 API 優先的開發人員導向工具，協助您將資安控管落實到 DevOps 流程當中。

✔ 更迅速的法規遵循

證明確實遵守各種法規要求，包括：GDPR、PCI DSS、HIPAA、NIST 以及 FedRAMP。

Trend Cloud One — Endpoint Security 與 Workload Security



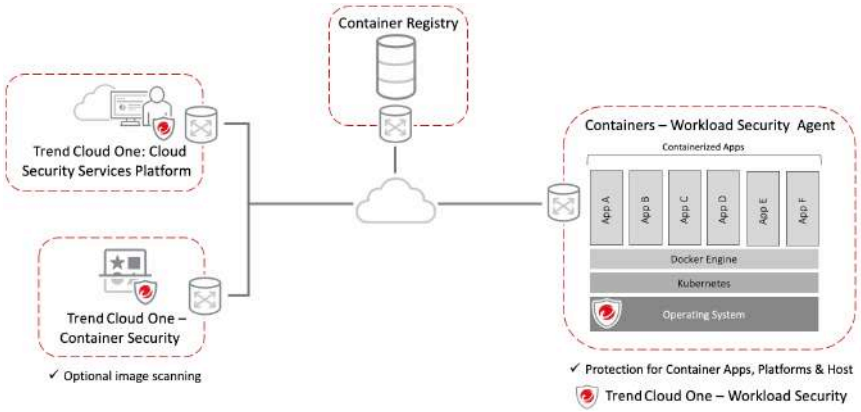
值得信賴的混合雲防護

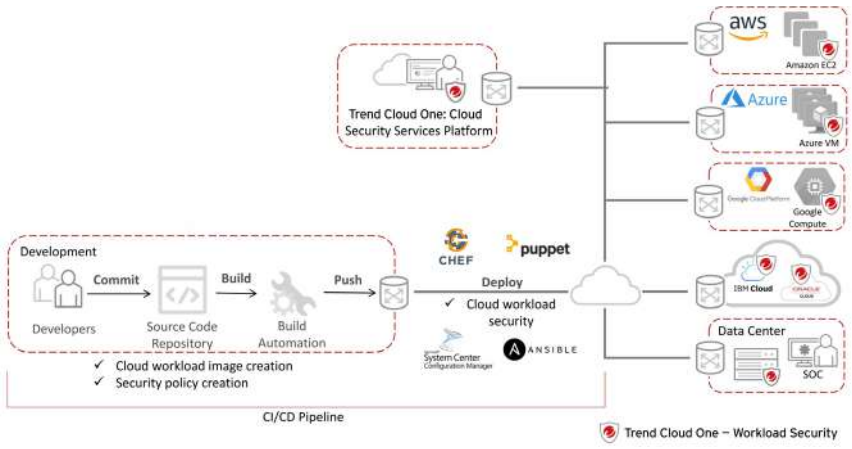
完整生命週期的容器防護

Workload Security 提供進階的執行時期容器防護。其多層式的防護能防範針對主機、容器平台 (Docker)、協調平台 (Kubernetes)、容器本身，甚至是針對容器化應用程式的攻擊。Workload Security 的設計包含了豐富完整的 API，可讓 IT 資安人員藉由自動化流程來保護容器，達成重要的資安控管。

DevOps 可利用資安程式碼將防護融入應用程式開發流程當中，減少在快速變遷或演變的基礎架構當中導入資安防護的阻力。

此外，還有 Trend Cloud One™ – Container Security 可讓您在建構流程當中搜尋容器映像內的漏洞、惡意程式、機密以及法規遵循問題，與執行時期的容器防護相輔相成。





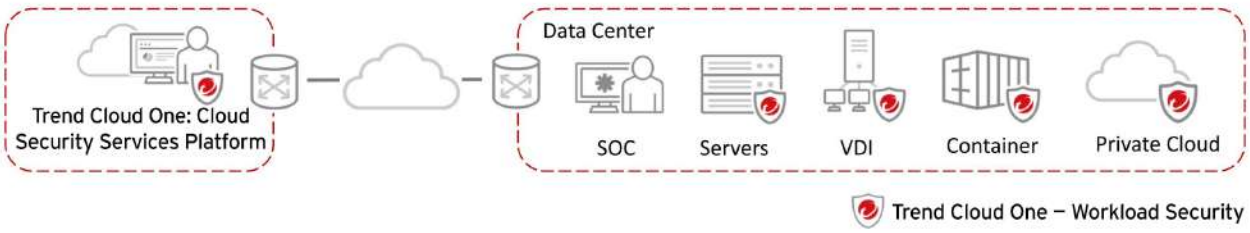
自動化雲端防護

Workload Security 能自動保護雲端工作負載，自動偵測各家雲端廠商的工作負載，包括：AWS、Microsoft Azure 及 Google Cloud Platform™ (GCP)。

其單一管理主控台能統一掌握所有工作負載與自動化防護的狀況，在多重雲端環境下享有一致且隨環境而調整的防護政策。此外，更透過部署腳本與 RESTful API 讓資安防護與您現有的工具整合，實現自動化的防護部署、政策管理、運作狀況檢查、合規報表等等。

虛擬化與資料中心防護

Workload Security 能為實體與虛擬伺服器提供進階防護，藉由自動化的政策管理讓多重環境的防護部署與管理變得輕鬆方便。Workload Security 能保護虛擬桌面和伺服器，防範零時差惡意程式，包括：勒索病毒、虛擬加密貨幣挖礦攻擊以及網路攻擊，並且盡可能減少資源利用效率不佳或緊急修補所帶來的營運衝擊。



以全球威脅研究為後盾的資安防護

我們遍布全球的 15 個研究中心以及世界各地超過 1 萬名的獨立研究人員，隨時掌握著全球威脅情勢的脈動。我們專精雲端與雲端原生應用程式的專家團隊，將其豐富的知識注入我們的產品當中，防範當前及未來的威脅。

布下天羅地網

我們隨時都在分析及發掘新的惡意程式、勒索病毒、惡意網址、幕後操縱 (C&C) 通訊位址以及駭客攻擊可能使用的網域。此外，我們也藉由 趨勢科技 Zero Day Initiative (ZDI)，這個領先市場的漏洞懸賞計畫，不斷發掘並負責任地揭露新的漏洞，協助我們的解決方案更快偵測各種應用程式及平台的威脅。

主要優勢

進階威脅防護

- 提供進階的資安控管，例如：入侵防護 (IPS)、一致性監控、機器學習、應用程式控管等等。
- 即時偵測及攔截威脅，幾乎不影響效能。
- 藉由多平台應用程式控管，偵測並防止未經授權的軟體執行。
- 利用 IPS 來防堵網站、企業應用程式及作業系統的已知和未知漏洞。
- 當偵測到可疑或惡意活動時發送警示通知並觸發主動防範措施。
- 檢查、偵測、防止經由 Transport Layer Security (TLS) 加密連線傳送的惡意內容而無須管理憑證和金鑰。
- 利用 IPS 所提供的虛擬修補來保護已終止支援的系統，確保老舊系統的安全，防範目前及未來的威脅。
- 持續追蹤網站信譽，藉由趨勢科技全球網域信譽評等資料庫的網站信譽情報來防止使用者瀏覽已遭感染的網站。
- 偵測及攔截殭屍網路與針對性攻擊的 C&C 通訊。
- 以領先市場的威脅研究及趨勢科技 Smart Protection Network™ 的威脅情報為後盾，提供更優異的防護來防範最新威脅。

支援並強化事件應變團隊：偵測及回應

搭配 Trend Vision One™ 來獲得 XDR 的優勢與專為伺服器、雲端工作負載及使用者端點而設計的整合式 EDR 功能。

- 接收經過優先次序過濾、可採取行動的警示以及完整的事件檢視。
- 調查 Linux 及 Microsoft Windows 端點與伺服器上的攻擊，找出問題根源與攻擊執行狀況，發掘攻擊範圍並直接採取回應。
- 透過多種方法來追蹤威脅，從強大的查詢功能到簡單的文字搜尋，主動找出駭客的攻擊手法或技巧，確認環境內的可疑活動。
- 利用趨勢科技的自動化情報或客製化情報掃描，持續搜尋是否有最新發現的入侵指標 (IoC) 。
- 搭配 Trend Vision One 來提供強化且交叉關聯的偵測、調查及回應能力，涵蓋電子郵件、網路、雲端、工作負載等防護層。
- 經由程式設計介面 (API) 與資安事件管理 (SIEM) 平台以及資安自動化協同及回應 (SOAR) 工具整合。
- 善用我們 7 天 24 小時的託管式偵測及回應 (MDR) 服務來補強您團隊的不足。

專為混合雲設計的全方位防護

- 藉由雲端及資料中心連動功能來自動發掘您混合雲環境當中執行的工作負載，讓您全面掌握並自動管理政策。
- 消除部署多套單一面向解決方案的成本，透過輕量化的單一代理程式與管理主控台，讓實體、 虛擬、雲端、容器及使用者端點環境皆享有一致的防護。
- 採用 Container Security 的進階建構時期映像與登錄掃描在流程的早期即加入資安防護，再搭配 Workload Security 的執行時期防護，就能保障容器完整生命週期的安全。
- 讓您的容器環境在各環節上都能確保安全，包括：主機、容器平台 (Docker)、協調平台 (Kubernetes)、容器本身，以及容器化應用程式。
- 採用相同的進階主機控管來保護您的容器主機，不論是實體、虛擬機器 (VM) 或雲端工作負載。
- 透過一致性監控和記錄檔檢查功能來監控 Docker 和 Kubernetes 平台是否出現任何遭到變更或攻擊的跡象。
- 採用容器漏洞防護 (藉由 IPS)、即時惡意程式防護，以及容器橫向網路流量檢查，來保護執行時期的容器。

實現符合成本效益的法規遵循

- 採用單一、整合又符合經濟效益的解決方案來達成重大法規遵循要求，例如：GDPR、PCI DSS、HIPAA、NIST 等等。
- 提供詳細記載已防止的攻擊與法規遵循狀態的稽核報表。
- 減少稽核的準備時間與人力。
- 支援內部合規計劃，提升內部網路活動的可視性。
- 協助整合各種工具，藉由強化的檔案一致性監控功能來達成法規遵循要求。

Workload 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 Micro Cloud One™ – Container Security：建構流程中的容器映像掃描。
- 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。

如需更多資訊，請至：trendmicro.com