IBM Cloud

保護容器平台

建立信任鏈

IBM

DevOps 挑戰：快速安全地進行創新

為了支援高度競爭市場中的業務目標，應用程式開發主管及團隊必須加快速度，針對不同裝置類型提供優質客戶體驗。因此，DevOps 團隊逐漸採用以容器為基礎的雲端平台以及敏捷的協同作業方式和工具鏈，以個別獨立但又互相交互之微服務來最大化雲端應用程式建立及運作的自動化。

在邁向以基於雲端的 DevOps 情境時，設定和維持絕佳安全性看似會增加麻煩，而且安全性絕對是不能忽略的。舉例來說，大多數的雲端平台都會使用 Docker 作為容器，而且容器會在共用的 Linux 核心上執行，這也承襲了其安全性挑戰。從社群下載，而且可在一個主機的 Linux 核心上取得有向上提報權限的未偵測到的異常容器軟體，可以開始透過阻斷服務攻擊 (DoS) 攻擊洩漏資料或另闢蹊徑。容器也可能會干擾其他容器，因為全部的容器都共享通道、程式庫及 binaries 等資源的 存取權限。

隨著自攜裝置 (BYOD) 模式的採用率逐漸提高，許多組織都喪失了企業端點的控制能力，從而削弱傳統企業管理範圍的能力。安全性現在必須隨工作負載提供，因為工作負載會在資料中心和雲端之間傳輸。

由於攻擊鏈 (闖入、鎖住、擴展、蒐集、洩漏) 維持不變，攻擊者的創意思維也會源源不絕地產生。時常佔據版面的重大違規反映的是安全性持續轉變的整體局勢：

- 攻擊者明白網路犯罪需要支付的代價，因而導致進階持續的威脅及其他攻擊不斷攀升，使得惡意程式迅速突變演化。
- 民族國家對於網路戰的能力也更加精細。在許多民族國家中，攻擊者已經使用國家資源來開發複雜的工具，同時還隱藏實際投入工作所花費的金額。

保護雲端平台的基礎挑戰當然會讓安全主管輾轉難眠。資訊安全長的目標是定義組織的安全性架構及要求，以便盡量降低風險和遵循法規之規範。部署必須是可稽核的。

這些要求可能使得資訊安全長與 AppDev 主管意見相左，因為 AppDev 主管需要可盡量提供自動化且可靈活整合至 DevOps 程序及管道 (若無法完全可見) 的安全性解決方案。

如何讓雲端平台高效且有效地 符合主要相關人員重視但衝突的需求？

建立信任鏈

解決方案是建立嵌入於硬體的信任鏈，驗證雲端平台中每個相關元件的完整性。 **真正的信任鏈會從主機晶片韌體開始並透過容器引擎和調度系統建立，因此可在應用程式生命週期期間保護所有關鍵的資料和工作負載。** 結果會是高度自動化且可靠的容器系統。

硬體是理想基礎，因為將矽芯片直接嵌入防禦方案，而使得駭客難以竄改程式。信任鏈會使用測量-及-驗證安全性模型建立，而且會對每個元件進行測量、驗證及啟動下一層級。此程序會延伸至容器引擎，建立信任範圍，而且會將測量結果儲存在主機上的可靠平台模組 (TPM)。不同伺服器上的證明軟體會依據已知的理想數值來驗證目前的測量值。容器調度程式會與證明伺服器進行通訊，以驗證工作節點和其上部署之任何容器鏡像的完整性。

關鍵要點

確定雲端平台支援受到原則管理的信任範圍，這對於自動化安全性至為關鍵。

圖 1 代表已嵌入硬體中的信任鏈，與將新工作節點新增至 Kubernetes 叢集時有關。 圖例中的數字會與此處描述的步驟 1 至 6 相對應。請記住，若要驗證開機主機上的測量值需要與個別證明伺服器上儲存的已知理想測量值進行比較。

1. 在工作節點上，TPM 硬體會驗證系統韌體，而且會測量和驗證包含選用 ROM 在內的 BIOS。之後會啟動 BIOS。
2. BIOS 會測量、驗證及啟動作業系統 (OS)。
3. 作業系統會測量、驗證及啟動 Docker 容器執行個體、Docker 外掛程式以及屬於信任運算基礎 (TCB) 的所有重要元件。
4. 藉由 Cloud Integrity Technology (CIT) 外掛程式，Kubernetes 主檔會透過證明伺服器驗證工作節點。證明也可納入檢查 Kubernetes 叢集的地理位置/範圍資訊，例如，不讓地理位置不適當之工作節點使用。
5. Kubernetes 主節點會將有效證明主機配置為現有叢集的一部分，其中包含指派容器。
6. 工作節點上的 Docker 引擎， 會透過加密連線與證明伺服器進行通訊， 而且會驗證容器鏡像的完整性並依據安全性原則加以檢查。

因為是由安全性原則驅動，整個容器平台會自動而且只會執行處於已知理想狀態的主機和容器。

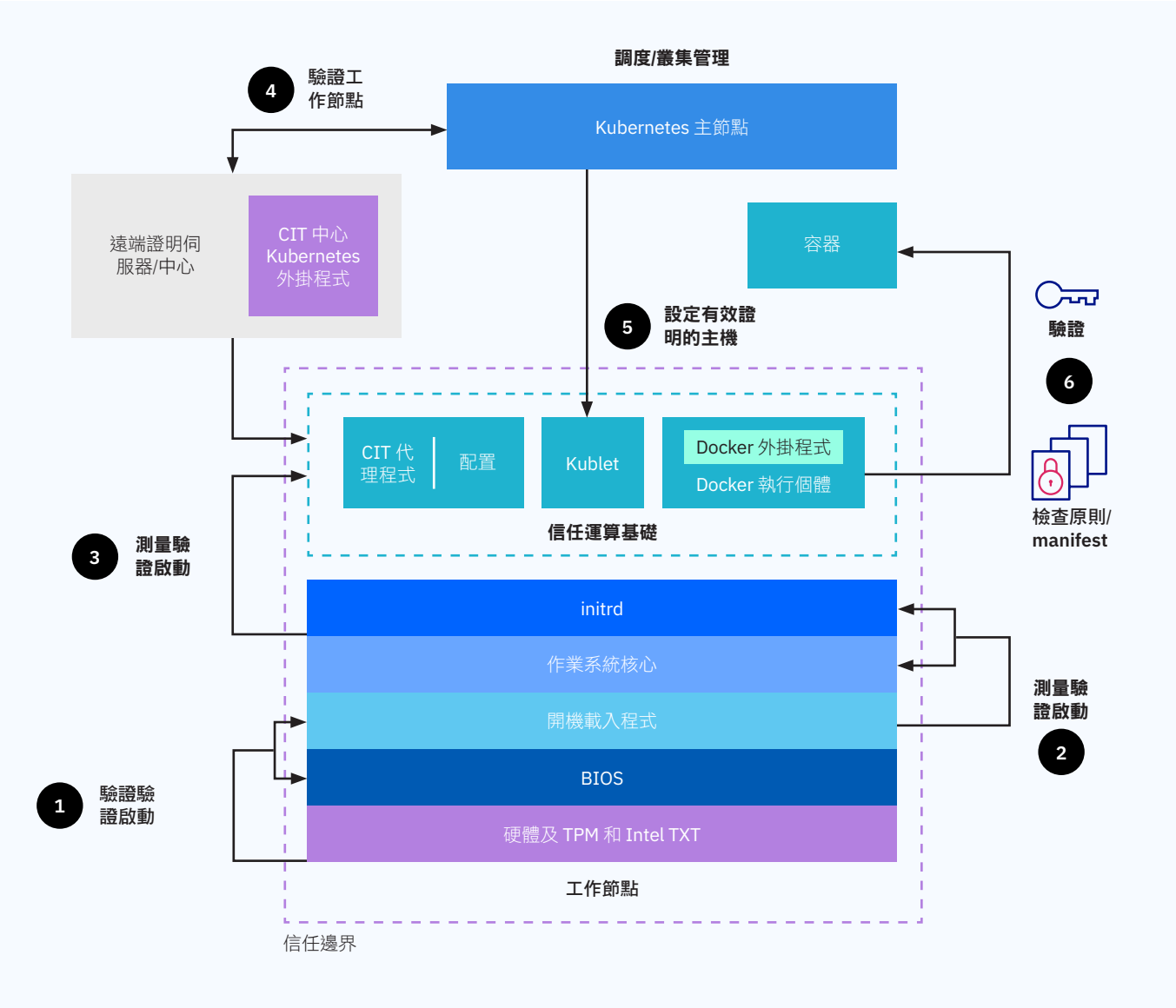


圖 1. 為容器啟用信任鏈的參考架構，可使用測量-及-驗證安全性模式作為延伸至 Kubernetes 調度等級的基礎。請參閱第 3 頁以取得六個步驟的描述。

啟用可靠的容器

Docker 此類的容器系統都有內建方法，而可針對系統的個別元素建立微範圍，以協助保護兩者之間的通訊內容。

若要評估容器化應用程式是否受到充分保護，請詢問雲端平台廠商關於 Docker 部署的下列面向：

是否會將軟體鏡像保存在私有目錄中 以 Docker Registry V2 為基礎的雲端平台可以為每個組織指派安全的私有鏡像目錄，其中只會依據指定的使用者及群組儲存和共用鏡像。將鏡像新增到私有目錄會與授權使用者建立或複製本地鏡像或是直接從公共儲存庫 (如 Docker Hub) 匯入鏡像有關。

Docker 部署是否會啟用鏡像加密？
加密可防止目錄中的鏡像遭到竄改。

Docker 類型是否是在運算主機上執行的類型，而且無需直接使用者存取權限進行設定？是否僅由服務廠商設定？
這兩個問題的答案應該都是「是」。直接存取其他客戶的主機可能會影響您容器的安全性。

所有 Docker 類型通訊端是否都受到傳輸層安全性 (TLS) 憑證之保護？
TLS 結合了公共金鑰加密、外部第三方驗證及每個工作階段加密的優勢。

是否允許任何有權限的 Docker 容器？
不允許有權限的容器可確保其他服務廠商客戶的容器不能存取運算節點上的硬碟，因為其中可能包含您的資料及應用程式。

從節點信任範圍移到可靠的雲端

因為運算節點已經成為建立信任鏈的焦點，而且因為每個節點都有自己的信任範圍，所有 Kubernetes 叢集及容量的所有成員就能開始保護 整體工作負載，然後再運算和傳輸 資料。

雲端廠商應說明和示範他們的信任技術。例如，Intel Trusted Execution Technology (Intel TXT)、符合規格 1.2 或 2.0 的任何 TPM，以及 Intel CIT 是廠商可能用於建立可靠雲端的既有技術。

- **Intel TXT** 會抵禦以軟體為基礎的攻擊，這類攻擊會透過毀損系統或 BIOS 程式碼來竊取機密資訊，或是修改平台的配置。
- **TPM** 是以硬體為基礎的安全性裝置，可儲存在測量-及-驗證安全性程序使用的測量值。有助於確保系統防竄改，然後才將系統控制能力釋放到軟體的下一個階段。
- **Intel CIT** 會建立信任的根目錄以提供原則導向的證明資訊，如此工作負載就能在驗證的硬體上執行，而且可遵循公有及私有雲環境之規範。

遠端證明是信任程序的重要步驟，這可將主機信任範圍延伸到容器調度層級。 Kubernetes 此類調度程式必須要能夠驗證運算節點的完整性，然後才能將容器部署到該節點。

若要提供遠端證明，雲端廠商可能使用 CIT 技術，這會在將雲端運算節點指派給容器環境時，新增進一步的驗證步驟。舉例來說，Intel CIT 會與 Intel TXT 搭配使用，以協助確定節點是防竄改且可靠的，容器叢集才會接受該節點。Intel CIT 也提供延伸，讓 DevOps 團隊輕鬆啟用工作負載的安全性原則，而且應用程式開發人員不需要處理原則。

關鍵要點

延伸節點層級信任範圍需要業界認可的加密解決方案。

透過隔離資源保護安全性

Kubernetes 調度程式也有助於保護叢集，方法是將服務-廠商-代管資源與組織帳戶的私有元件區隔開來（圖 2）：

- Kubernetes 專屬主節點及包含控制鏡像存取權限之私有鏡像目錄就能在代管網路中執行。
- 可以將包含容器化工作負載容量的 Kubernetes 工作節點，部署在由組織（而非廠商）控制之專屬網路上的組織基礎架構帳戶。

這個方法可賦予 DevOps 團隊高階控制能力並提供資訊安全長需要的隔離。在主要及工作人員節點之間的通訊 會透過加密網路連線進行，以及提供加密及金鑰的 Kubernetes； 輸入控制器會自動產生 TLS 憑證以存取 Kubernetes 容量。 使用 Kubernetes 基於角色的存取控制， 組織就能透對叢集中的資源設定精細的限制。

原則導向自動化

Kubernetes 可讓 DevOps 團隊將系統功能分成非常小的原子元素，其中每個元素都能嵌入基礎信任架構，以協助確保每個元素都能依據原則進行存取及通訊。隨著團隊建立複雜的微服務架構，原則導向自動化就能控制存取權限及路由，因此可針對個別應用程式及其元件輕鬆縮放規模。

Calico 及 Istio 是 Kubernetes 生態系統的兩個重要部分，可協助確保應用程式及工作負荷載安全性。Calico 簡化對於將 IP 位址指派至運算節點中之工作負載的管理作業，以及每個運算節點中的程式存取控制清單有助於增強安全性原則。透過原則定義設定並透過標籤強制執行， Istio 可針對 Kubernetes 容量或叢集的微服務之間，提供以憑證為基礎的控制能力。

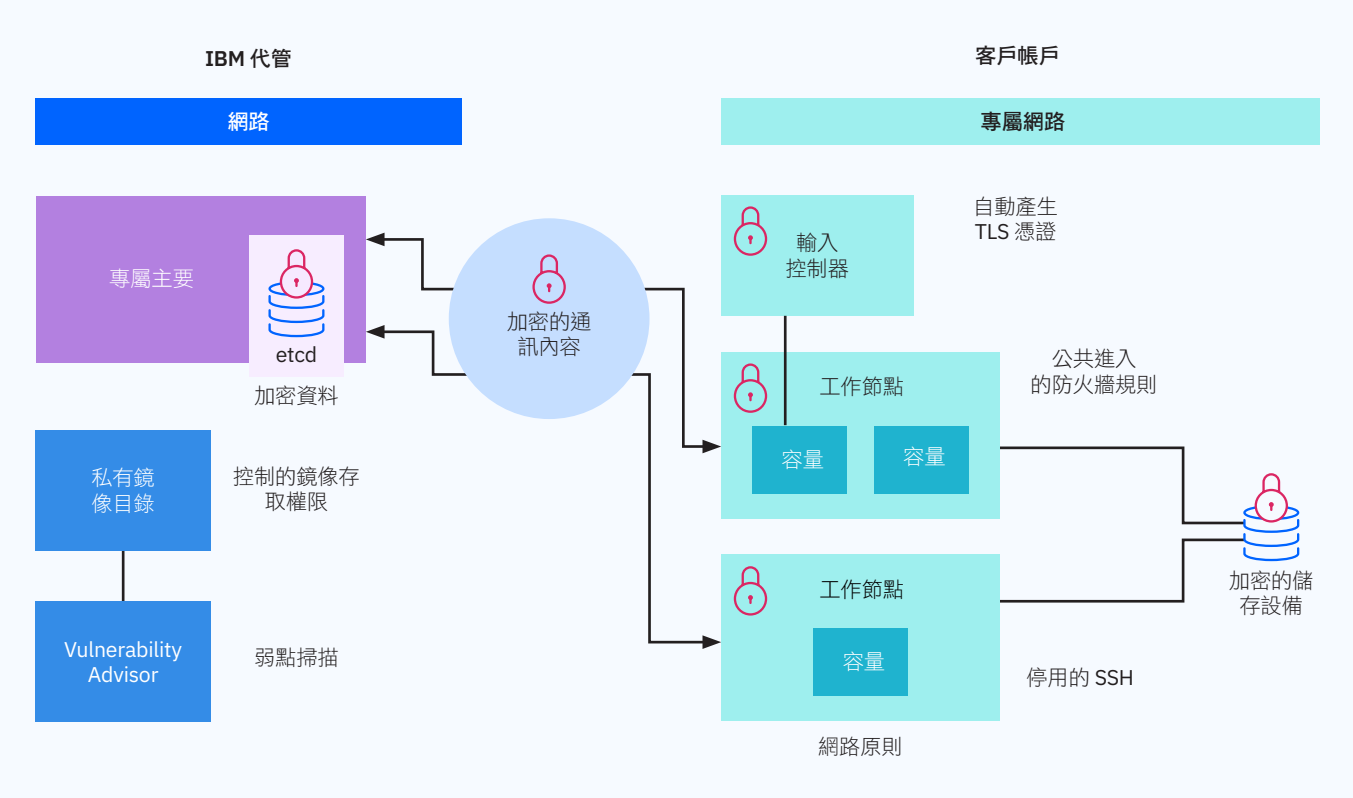


圖 2. 分隔廠商管理及客戶管理的叢集元素。

延伸信任鏈的優勢

將遠端證明及加密與安全性原則緊密結合的完整部署信任鏈，都能讓這些重要功能管理容器、應用程式及工作負載：

- **透明度及可擴充性：**由於可透過信任鏈進行自動化，DevOps 團隊就能任意地毫無阻礙地迅速作業。他們只能依據可靠地容器系統評估 其測量值來管理安全性原則。有了適當的配置之後，會依據即時流量以自動調整應用程式資源而增加或減少調度。
- **地理工作負載原則驗證：**智慧容器調度僅限制移動到核准的位置。
- **容器完整性保證：**移動容器時，會檢查容器以確保在流程中不會進行竄改作業。驗證的移動容器會與原始建立的容器相同。
- **機密資料的安全性：**只能解密特定位置中核准之伺服器上的加密容器。
- **簡化合規性控制及報告：**中繼資料稽核軌跡提供可見性及可稽核證據，可讓關鍵容器工作負載在可靠的伺服器上執行。

關鍵要點

當您的團隊評估雲端平台時，請廠商說明如何針對託管應用程式的技術足跡建立和維持信任。這是您組織業務吸引客戶和保留重要資料的基礎。

案例焦點：減緩 GDPR 憂慮

假如您的客戶位於歐洲，您可能會為即將面臨的潛在龐大責任而擔憂，因為歐盟「一般資料保護規範」(GDPR) 即將生效。因為主權要求及其他法規代表特定資料種類無法離開產生資料的國家/地區，您需要：

- 強力保證當您需要特定區域性的工作負載時，這些工作負載無法也不會進入其他地區。
- 受管工作負載的加密金鑰，如此一來，除了您要放置工作負載的地區以外，就不能在任何地方解密資料。

當您建立置入硬體的信任鏈之後，您可以將對於維持完整性、管理金鑰及保證工作負載的區域性至微關鍵的所有元素緊密結合。而且您可以透過原則推動這項信任關係，而且可隨應用程式部署擴充安全性。

掃描靜態及即時容器

開始使用 Docker 容器很簡單：開發人員可以下載在 Docker Hub 上公開使用的任何容器鏡像，例如，避免或大幅降低準備鏡像堆疊部分內容的時間。問題是在部署之前，無法確定該鏡像中有何內容。因此，必要實務是先掃描每個鏡像，然後才將之適當釋放到 DevOps 管道。雲端平台必須提供有效率的方法來執行此操作。舉例來說，IBM® Cloud Container Service 提供的 Vulnerability Advisor (VA) 系統，可同時進行靜態及即時的容器掃描 (圖 3)。VA 會檢查雲端客戶私有目錄中每個鏡像的每個圖層，以偵測是否存有弱點或惡意程式，然後再部署鏡像。然而，因為單純掃描目錄鏡像可能會錯過一些問題 (例如，從靜態鏡像到部署容器的漂移)，VA 也會掃描執行的容器是否有異常情形。此外，也會以分層式警示提供建議。

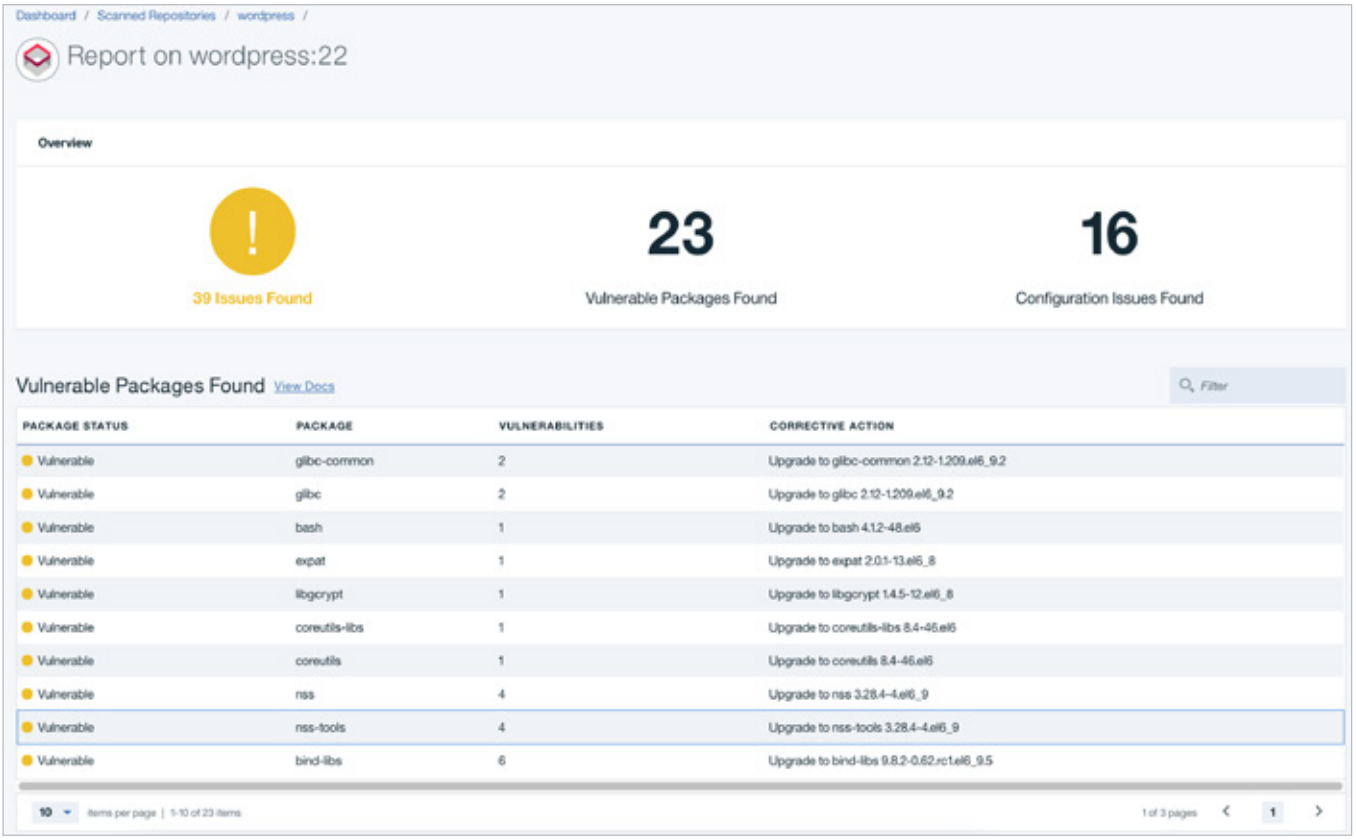


圖 3. VA 會與 X-Force 整合，以依據已知修正程式之攻擊向量、複雜性及可用性而對弱點評分。

雲端隔離技術

以晶片為基礎的技術代表，部署信任鏈需要在支援 VPN 存取權限之專屬主機上部署的能力。所有容器應該都以運算主機上的獨立、隔離程序形式執行，而且應該要限制對其資源的存取權限。

使用最佳化運算主機核心，雲端廠商應該要能夠自動限制可在任一運算主機上執行的執行緒及程序的總數。這項最佳化可確保主機不會超載 (這可能會影響您的應用程式效能)，為您帶來優勢。

服務廠商也應該持續監控運算主機，以控制和補救 fork 炸彈和其他程序層級的 DoS 攻擊。管理資料夾、檔案、網路網域及權限以建立和變更資料之存取權限的安全性控制能力，應該在 Linux 核心層級開始。

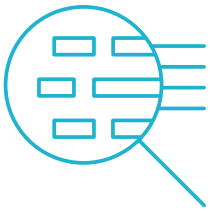
雲端安全性的可見性

維運工程師通常會仔細檢查內部部署資源，並且對於以雲端為基礎的容器化工作負載套用相同的洞察。為了提供這樣的可見性，雲端廠商應該自動記錄所有使用者及管理存取權限，無論是依據組織或廠商而定。內建雲端活動追蹤程式可以建立存取所有平台及服務的軌跡，而可讓客戶組織存取相關日誌檔。

確定您已經選擇將所有日誌檔及事件整合至內部部署安全性作業中心 (SOC) 資訊和事件管理 (SIEM) 系統。某些雲端服務廠商提供包含事件管理及報告功能之安全性監控、安全性警示的即時分析等額外服務，以及混合部署之間的整合式檢視。

舉例來說，IBM QRadar® 是全方位的 SIEM 解決方案，可提供一組能隨組織需求擴充的安全性智慧功能。包含針對威脅模式提供的機器學習功能訓練，可建構智慧安全性免疫系統。

探索 Vulnerability Advisor



IBM Vulnerability Advisor 的特性包含下列項目：

- **原則違規設定：**藉由 VA，管理員就能依據三種類型的鏡像失敗情形來設定鏡像部署原則：包含已知弱點的已安裝套件；已啟用遠端登入；以及某些使用者可輕鬆猜到密碼並啟用的遠端登入。
- **最佳實務：**VA 目前會依據 ISO 27000 (包含密碼最短有效時間和密碼長度下限等設定) 來檢查 26 個規則。
- **安全性錯誤配置偵測：**VA 會針對每個錯誤配置問題設定旗標、提供描述並建議補救動作。
- **與 IBM X-Force® 整合：**VA 會從五個第三方來源抽取安全性情報，而且會使用已知修正程式的攻擊向數、複雜性及可用性對每個弱點進行評分。評分系統 (嚴重、高、普通或低) 可協助管理員快速瞭解弱點的嚴重性並排列補救動作的優先順序。

為業務需求提供服務的端對端安全性

容器技術為應用程式開發團隊提供服務， 方法是簡化及增加協同作業在雲端環境中的速度。但為了提供那些優勢，雲端平台必須符合資訊安全長的安全性要求，而不會產生不當問題。因此，為了符合企業目標，DevOps 團隊需要透過自動化安全性部署資訊安全長要求的原則。

植入硬體的信任鏈是實現此目標的有效基礎。其中應該包含可確保信任容器及強制執行安全性原則能管理容器部署的技術。信任鏈架構設計旨在符合安全性及迅速創新的迫切需求：

- 安全性主管可以制定安全性原則並在建立或移動每個容器時自動套用此原則。
- 序列中的每個步驟都會自動化進行，因此可讓 DevOps 團隊快速建立和部署應用程式，而不需要停下來新增安全性元件。

此架構可為資料及應用程式提供從硬體層級到雲端平台之容器調度層的保護，因此可協助組織遵循歐盟「一般資料保護規範」(EU GDPR)、美國聯邦風險及授權管理計畫 (FedRAMP) 及美國醫療保險流通與責任法案 (HIPAA) 之規範。組織會定義其產業確切所需的原則並保證擔保的元素。`

IBM 觀點

信任鏈的創新是 IBM 及其合作夥伴的關鍵重點。IBM 和 Intel 長期合作並致力於開發信任鏈安全性解決方案，而現在則將專業知識運用於以容器為基礎的產品。目標：協助組織透過安全且敏捷的方法部署容器，為今日的創新者提供他們需要和值得擁有的開發彈性和先進的微服務架構。

IBM Cloud 可為團隊提供隨時可用的開放原始碼工具，以自動化進行部署及管理。而且，如果客戶想要在多個雲端上部署工作負載，雲端平台必須讓他們在多雲端環境之間一致地使用相同工具。可能的話，容器安全性的未來是開放、敏捷、自動化的，而且具備強大且智慧的防禦能力。

可能的話，容器安全性的未來是開放、敏捷、自動化的，而且具備強大且智慧的防禦能力。

如需更多資訊

若要深入瞭解如何為容器安全性建立信任鏈，
請造訪 ibm.com/cloud/container-service

對於安全性和 DevOps 有興趣？請加入我們的 Slack 頻道並和IBM Cloud Container Service 產品團隊的開發人員交換意見。

保持聯繫，掌握動態

IBM Cloud Container Service
IBM Cloud 部落格

關注我們

@IBMcloud
Facebook

與我們交流

LinkedIn
YouTube

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722

美國印製 2018 年 2 月