Prisma Cloud Compute 版
概覽

雲端原生安全挑戰

傳統的安全工具和方法不適用於保護與基礎結構無關、開發人員導向型、多雲端模式的雲端原生應用程式。這是因為：

- 開發人員和 DevOps 團隊對於建立和部署雲端原生應用程式而言極為重要，這些人的作業通常不受到傳統安全性的保護。這需要與開發人員主導的基礎結構和工具整合的安全性。
- 企業使用的運算選項比以往更多，跨越混合雲和多雲端部署，並結合使用主機虛擬機器 (VM)、容器、Kubernetes®、容器即服務 (CaaS) 和無伺服器功能。
- 雲端原生環境不斷發生巨大變化。安全團隊需要透過自動化來保護組織使用的數量不斷增加的千變萬化的微服務。

跨主機、容器和無伺服器的雲端工作負載防護

Prisma™ Cloud Compute Edition 為現代企業提供雲端工作負載防護平台 (CWPP)，可在整個軟體生命週期中，為任何雲端中的主機、容器和無伺服器部署提供全面保護。Prisma Cloud Compute Edition 是雲端原生且支援 API，無論採用何種基礎運算技術以及在何種雲端執行，都可以保護您所有的工作負載。

功能

為了全面保護，Prisma Cloud Compute Edition 提供：

- **弱點管理**：在應用程式生命週期的每個階段，透過無與倫比的弱點偵測、瞭解和防禦，享受從開發到生產的安全性。
- **合規性**：輕鬆實作並維持 Docker、Kubernetes 和 Linux CIS 基準的合規性，以及外部合規性制度和自訂要求，包括業界首次對 Istio® 服務網進行合規性檢查。
- **CI/CD 安全性**：將安全性直接整合到持續整合 (CI) 流程中，以便投入生產之前發現並解決問題。
- **執行階段防禦**：機器學習可為每個應用程式的每個版本自動建立最低權限、加入允許清單的執行階段模型，藉以大規模地保護護您的環境。
- **網路應用程式和 API 安全性**：防禦任何公有雲或私有雲中的第 7 層和 OWASP 前 10 大威脅。
- **存取控制**：針對跨基礎主機、Docker 和 Kubernetes 的雲端工作負載和雲端原生應用程式，建立並監控存取控制措施，同時與身分和存取管理 (IAM) 及密碼管理工具，以及其他核心技術整合。

運作方式

Prisma Cloud Compute Edition 提供彈性的部署選項，無論您選擇在哪裡部署，都可以保護您的工作負載和應用程式。Defender (在您環境中部署的代理程式) 可保護獨立的虛擬機器、Docker 容器、Kubernetes 叢集、CaaS、Pivotal Application Service 上的 PaaS 應用程式，以及無伺服器應用程式。Defender 透過將應用程式行為列入允許清單並防止發生異常動作來提供保護。深層防禦將核心的雲端原生防火牆與執行階段防禦結合在一起，以保護東西向流量，並將機器學習用於已知的應用程式行為。

Prisma Cloud Compute Edition 透過與任何持續整合程序、Docker 登錄、程式碼儲存庫或生產環境整合，透過強大的風險因素和優先順序持續監控風險，藉以在整個軟體生命週期內提供弱點管理和合規性。企業級存取控制功能可以跨運算基礎結構、密碼、Kubernetes 稽核和 IAM 工具，監管所有雲端資源。

Prisma Cloud Compute 版
概覽

Prisma Cloud Compute Edition 是透過容器映像提供的自我託管選項，客戶可以在任何環境 (無論是公有雲、私有雲還是混合雲環境，包括完全氣隙式環境) 中自行部署和管理。如需有關 SaaS 部署模型的詳細資訊，請參閱 Prisma Cloud：概覽。

主要優點

- **可採用您喜歡的任何雲端原生技術**。保證您的基礎結構決策能夠與時俱進。為任何指定應用程式元件選擇適當的工作負載，並知道您的安全平台可以提供萬全的保護。
- **在雲端原生環境中，根據脈絡，確定風險的優先順序**。利用整個雲端原生基礎結構以及整個軟體生命週期中的持續弱點情報和風險優先順序，包括具有執行階段威脅數據的即時連線圖。
- **以 DevOps 速度，將安全性自動化**。使開發人員和 DevOps 團隊能夠盡快部署，以便為客戶提供商業價值，並改善安全成果。

若要深入瞭解 Prisma Cloud，請造訪我們的網站。

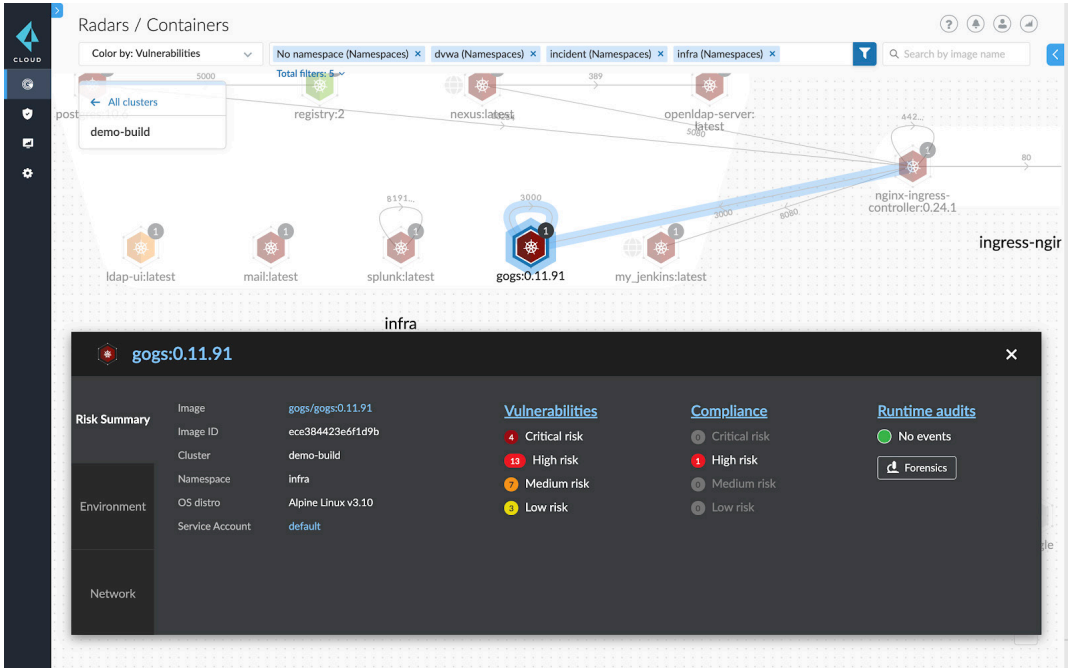

圖 1：容器的 Prisma Cloud Radar 以及整合弱點、合規性和執行階段詳細資料