Prisma Cloud
概覽

從程式碼到雲端保護應用程式

Prisma® Cloud 是雲端原生應用程式保護平台 (CNAPP)，能夠保護任何公用雲端、私人雲端、混合雲端或多雲端環境中的應用程式。與單點產品的集合不同，Prisma Cloud 將廣泛的安全功能整合到單一平台中，以提供統一且同級最佳的安全性。我們方法的好處包括降低風險、減少入侵、促進開發安全協作、提高效率，以及改善合規性和安全狀況。

風險防禦

防止風險和錯誤設定進入生產環境。

可視性和控制

對於您的雲端環境建立連續可視性與控制。

執行階段防護

為雲端工作負載、Web 應用程式和 API 提供即時保護。

圖 1：Prisma Cloud 的統一程式碼到雲端™ 方法

Prisma Cloud 使用案例

風險防禦

透過設計將測試左移並保護應用程式。Prisma Cloud 與工程生態系統整合，防止風險和錯誤設定進入生產環境，藉以提供：

- **基礎結構即程式碼 (IaC) 安全性：**在 Terraform、CloudFormation、ARM、Kubernetes 和其他 IaC 範本中識別及修正錯誤設定。
- **密碼安全性：**尋找並保護儲存庫和 CI/CD 管道中所有檔案中暴露的和易受攻擊的密碼。
- **CI/CD 安全性：**強化 CI/CD 管道、縮小攻擊範圍並保護您的應用程式開發環境。
- **軟體組成分析：**透過脈絡感知優先順序排定解決開放原始碼弱點和授權合規性問題。

可視性與控制

獲得對整個雲端環境中的雲端錯誤設定、身分和存取、數據、弱點和 API 端點的持續可視性和控制。Prisma Cloud 可保護雲端基礎結構，藉以提供：

- **雲端安全狀況管理 (CSPM)：**監控狀況、偵測和補救風險，並且保持合規性。
- **雲端基礎結構權限 (CIEM)：**跨多雲端環境控制權限。

- **無代理程式工作負載掃描：**掃描主機、容器、Kubernetes 和無伺服器以尋找弱點和威脅。
- **雲端數據安全性：**識別敏感數據並掃描公用雲端儲存中的惡意軟體。
- **API 可視性：**跨雲端原生應用程式發現、分析和保護 API。
- **雲端發現和暴露管理：**提高對暴露在網際網路上的未知、未受管理雲端資產的可視性和控制。

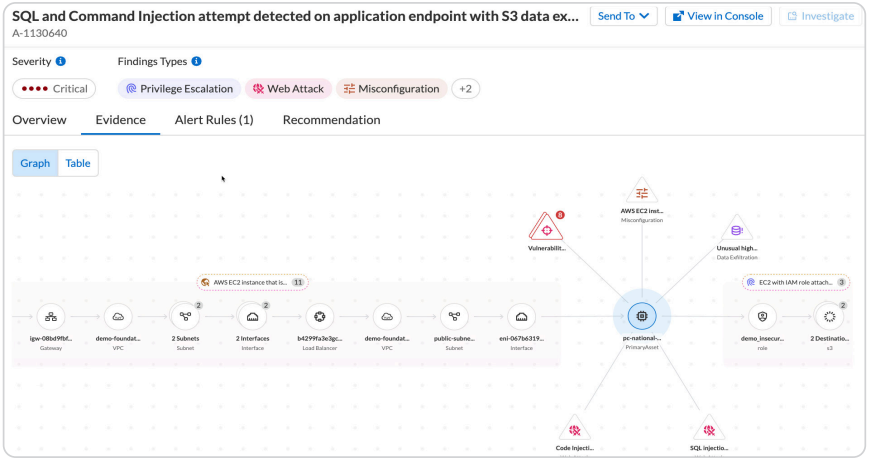

圖 2：攻擊路徑分析

Prisma Cloud
概覽

執行階段保護

在執行階段阻止入侵並保護應用程式免受攻擊。Prisma Cloud 跨公用雲端和私人雲端提供威脅防護，其中包括：

- **雲端威脅偵測：**偵測多雲端環境中的進階威脅、零時差攻擊和異常。
- **主機安全性：**保護任何公用雲端或私人雲端的雲端虛擬機器。
- **容器安全性：**在任何公用雲端或私人雲端上保護容器和 Kubernetes 平台。
- **無伺服器安全性：**在整個應用程式生命週期中保護無伺服器功能。
- **Web 應用程式和 API 安全性：**保護任何公用雲端和私人雲端中的 Web 應用程式和 API。

程式碼到雲端智慧

我們獨特的方法由程式碼到雲端智慧提供支援，透過應用程式執行階段連接來自開發人員環境的見解，藉以降低風險並防止入侵。Prisma Cloud 將警示置於脈絡中，確定關鍵風險的優先順序，並提供補救指南。

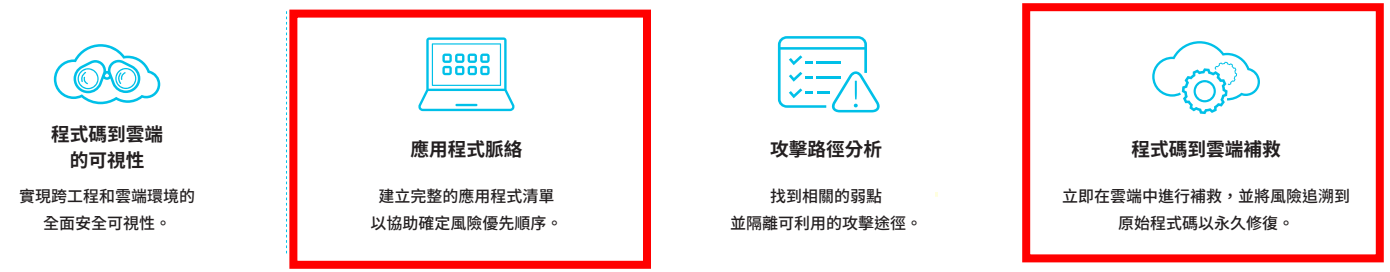

圖 3：程式碼到雲端智慧

「有了 Palo Alto Networks，一切都變得如此簡單。原生整合相當緊密，可視性相當的完整，而且自動處理絕大多數監控。這也完全不會影響我們的資源。」

– Oussama Benzaouia，Teads 資訊安全長

閱讀完整案例研究。

「Palo Alto Networks 產品組合在各個層面上都有意義。我們不依賴單點安全解決方案，而是擁有一套經過驗證的最佳實務、互連安全技術。我們的團隊可以專注於增值任務，確信關鍵的安全程序在後台執行，保護我們新的數位基礎結構。」

– Bob Bowden，Registers of Scotland 安全架構師

閱讀完整案例研究。