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。

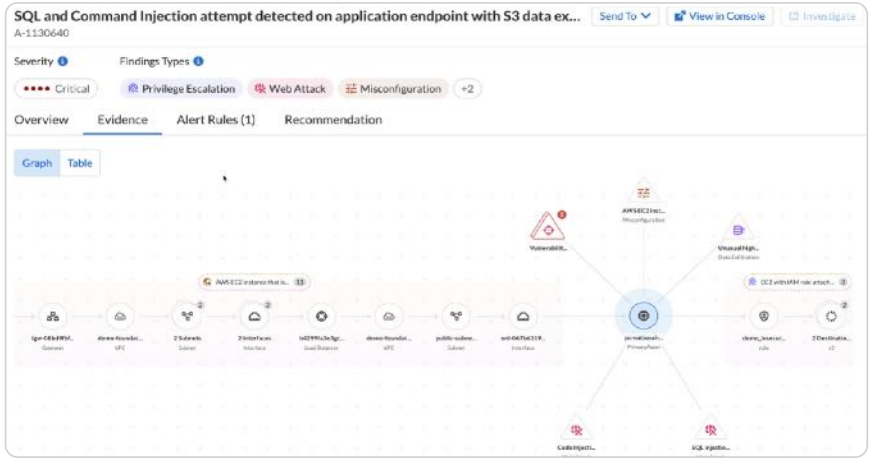

圖 2：攻擊路徑分析

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。

程式碼到雲端的可視性

實現跨工程和雲端環境的全面安全可視性。

應用程式脈絡

建立完整的應用程式清單以協助確定風險優先順序。

攻擊路徑分析

找到相關的弱點並隔離可利用的攻擊途徑。

程式碼到雲端補救

立即在雲端中進行補救，並將風險追溯到原始程式碼以永久修復。

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。

雲端安全狀況管理

維護應用程式、工作負載和數據的合規性

Prisma Cloud 可降低複雜度，並保護混合雲端和多雲端環境的資源。我們全面的雲端原生應用程式保護平台 (CNAPP) 獲得全球 1,900 多家領先企業的信賴，每天保護超過 70 億個雲端資源並且分析超過一兆個事件。Prisma Cloud 可消除盲點並偵測其他工具遺漏的威脅，為使用者提供完整的可視性、持續的威脅偵測和自動化回應。

現今多雲端現實的全面安全狀況管理

有效的雲端安全性需要對每個已部署的資源掌握完整的可視性，並對設定和合規性狀態抱持絕對的信心。隨著企業持續採用雲端原生方法並獲得多雲端架構的彈性，將來自不同傳統工具的安全數據加以整合成為相當大的障礙。DevOps 和安全團隊需要 Prisma Cloud 之類的單一整合解決方案。

該平台採用獨特的雲端安全狀況管理 (CSPM) 方法，不侷限於合規性或設定管理。來自 30 多個數據來源的弱點情報可提供對於關鍵安全問題的即時明確性，而整個開發管道的控制可防止不安全的設定進入生產環境。

CSPM 功能

可視性、合規性和監管

雲端資產目錄

Prisma Cloud 提供全面的可視性，並且可控制每個已部署的資源所呈現的安全狀況。雖然某些解決方案僅彙總資產數據，不過 Prisma Cloud 會分析並規範化不同的數據來源，藉以提供絕佳的風險明確性。

Amazon EFS	aws	24	0	24	0	24	0	0%
AWS Secrets Manager	aws	7	7	0	0	0	0	100%
Amazon EKS	aws	1	0	1	0	1	0	0%
Amazon SQS	aws	5	0	5	0	5	0	0%
Amazon S3	aws	66	0	66	66	0	0	0%
Azure Virtual Network	Azure	120	87	33	18	15	0	73%
Azure Network Watcher	Azure	31	31	0	0	0	0	100%
Azure Resource Manager	Azure	9	7	2	0	0	2	78%
Azure Policy	Azure	3	3	0	0	0	0	100%
Azure SQL Database	Azure	2	0	2	2	0	0	0%
Azure Compute	Azure	31	17	14	5	9	0	55%
Azure Storage	Azure	13	0	13	1	12	0	0%
Azure App Service	Azure	1	1	0	0	0	0	100%
Azure Security Center	Azure	2	0	2	0	2	0	0%
Google Resource Manager	Google	114	91	23	12	11	0	80%

圖 1：資產目錄

合規性監控和報告

Prisma Cloud 持續監控雲端合規性狀況，並支援從單一控制台進行一鍵式報告。包含超過 65 個立即可用的合規性框架，您也可以建立其他自訂框架。

圖 2：合規性儀表板

脈絡驅動的風險優先順序

不同於只注意個別錯誤配置的孤立工具，Prisma Cloud 關聯廣泛的資訊集以協助確定風險優先順序。這個平台針對建立潛在攻擊路徑的組合分析錯誤設定、網路暴露、過度權限和弱點。這種基於風險的分析運用 Prisma Cloud 脈絡引擎來識別雲端中的多個弱點，這些弱點會在精密攻擊中遭利用。

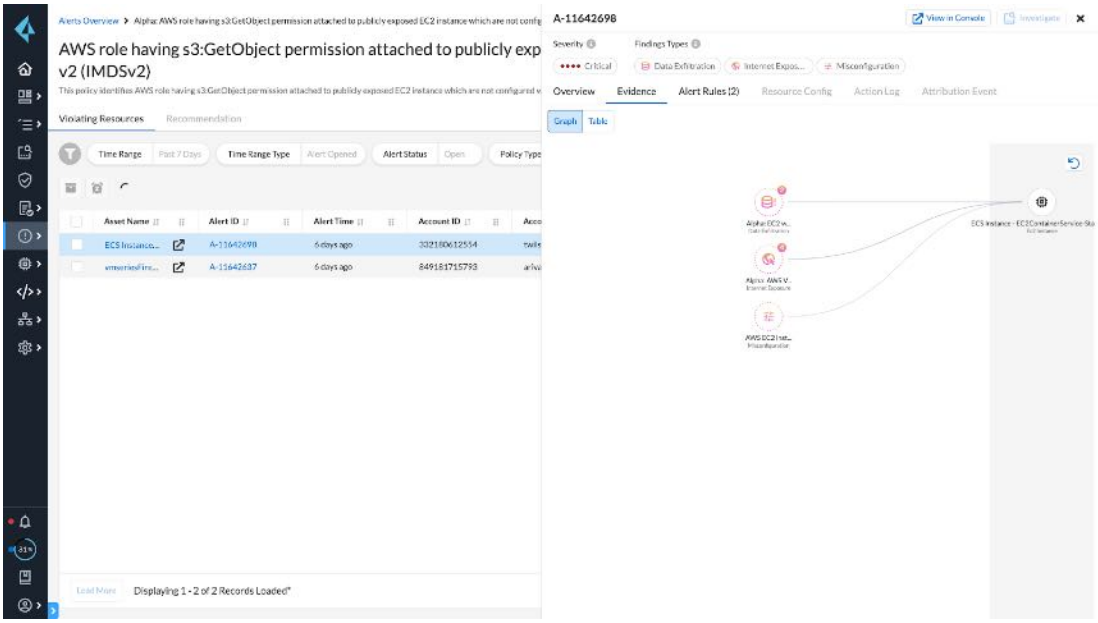

圖 3：攻擊路徑警示調查

威脅偵測

使用者與實體行為分析 (UEBA)

Prisma Cloud 分析數百萬個稽核事件，然後使用機器學習 (ML) 來偵測異常活動，這些異常活動可能表示帳戶入侵、內部威脅、存取金鑰遭竊以及其他潛在的惡意使用者活動。

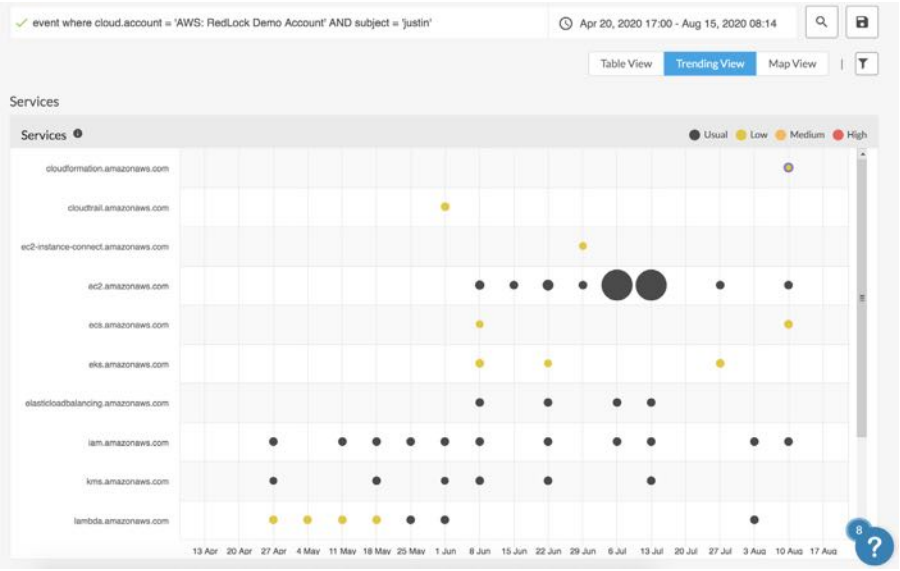

圖 4：異常活動追蹤器

網路異常和威脅偵測

Prisma Cloud 會監控網路行為並且運用機器學習和進階威脅摘要來偵測網路異常和威脅。藉由 Prisma Cloud，您可以偵測連接埠掃描和連接埠探測活動，這些活動會探測伺服器或主機的開放連接埠，以及隱藏在網域名稱系統 (DNS) 流量中的威脅，例如網域產生演算法 (DGA) 和加密貨幣採礦活動。

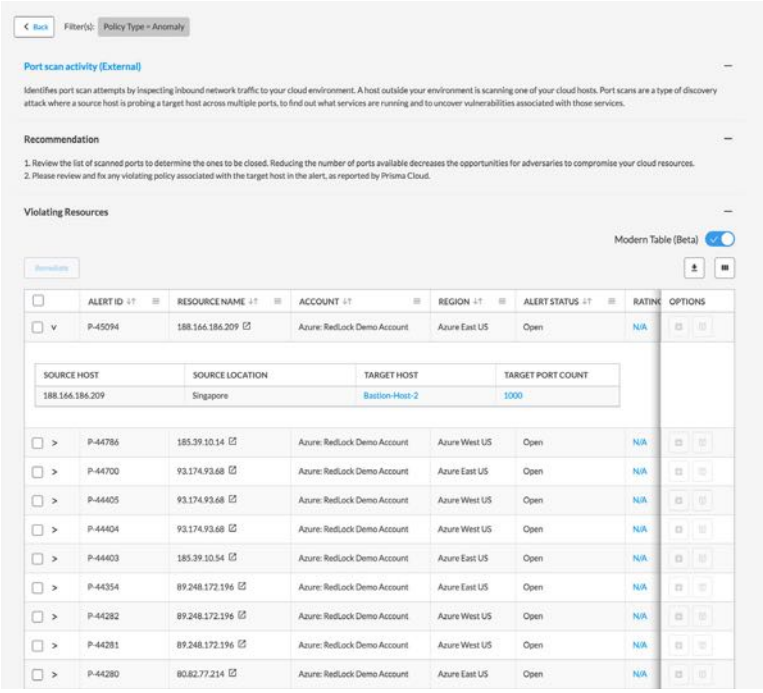

圖 5：連接埠掃描活動詳細資料

自動化調查與回應

Prisma Cloud 提供自動補救、詳細的鑑識和關聯功能。來自工作負載、網路、使用者活動、數據和設定的深入見解可加速事件調查與回應。

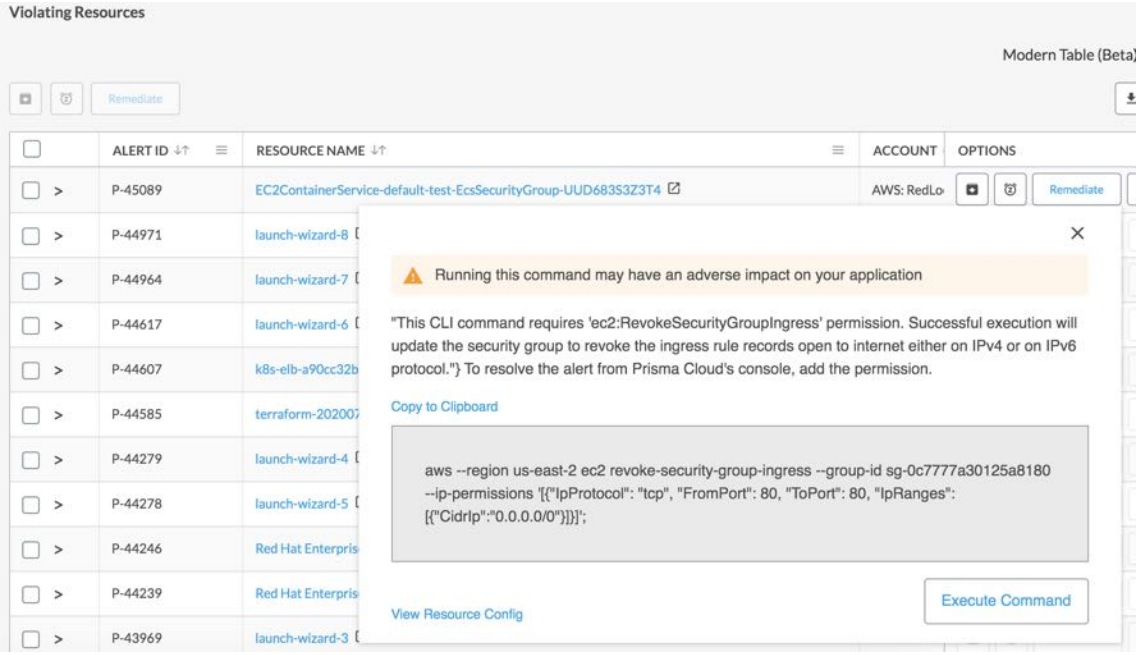

圖 6：自動化調查詳細資料

數據安全性

數據可視性與分類

Prisma Cloud 提供對 Amazon S3 和 Microsoft Azure Storage 陣列和物件的完整可視性，包括按區域、擁有者和暴露層級的內容。您可以微調數據識別碼 (例如駕照、社會保險號碼、信用卡號或其他格式) 以識別和監控敏感內容。

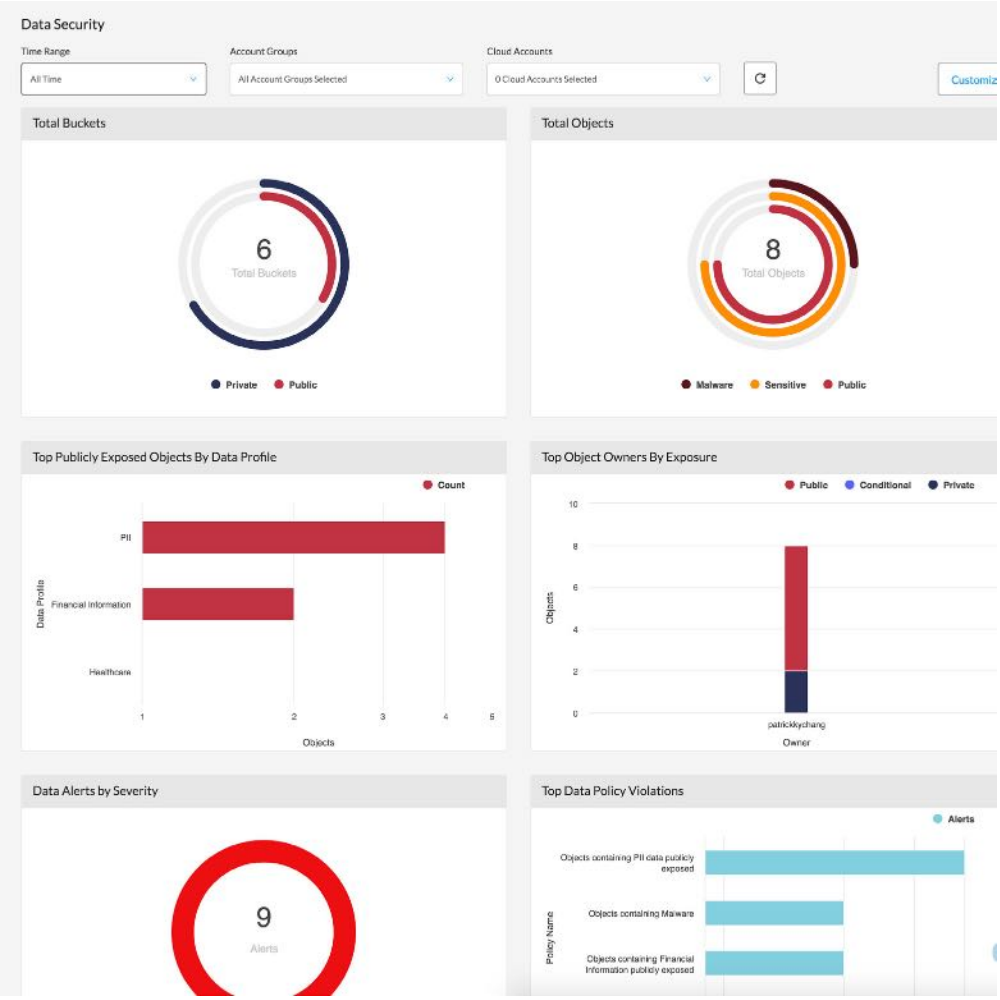

圖 7：S3 數據安全儀表板

數據監管

Prisma Cloud 包含特定的數據政策，可按照數據分類和暴露/檔案類型迅速確定您的風險狀況。按照需要啟用或停用數據合規性評估設定檔 (例如 PCI、GDPR、SOC 2 和 HIPAA)，只需按一下即可產生可稽核的報告。

惡意軟體偵測

Prisma Cloud 運用 WildFire 惡意軟體防禦服務來標記包含惡意軟體的任何物件，藉以協助使用者識別並防禦已入侵 S3 陣列和 Azure Storage Blob 且基於已知和未知檔案的威脅。

警示和補救

Prisma Cloud 會按照數據分類、數據暴露和檔案類型自動為每個物件產生警示。分析人員可以對警示採取動作，藉此迅速補救暴露情況、標記各個 DevOps 團隊違規行為，並迅速刪除包含惡意軟體的任何物件。

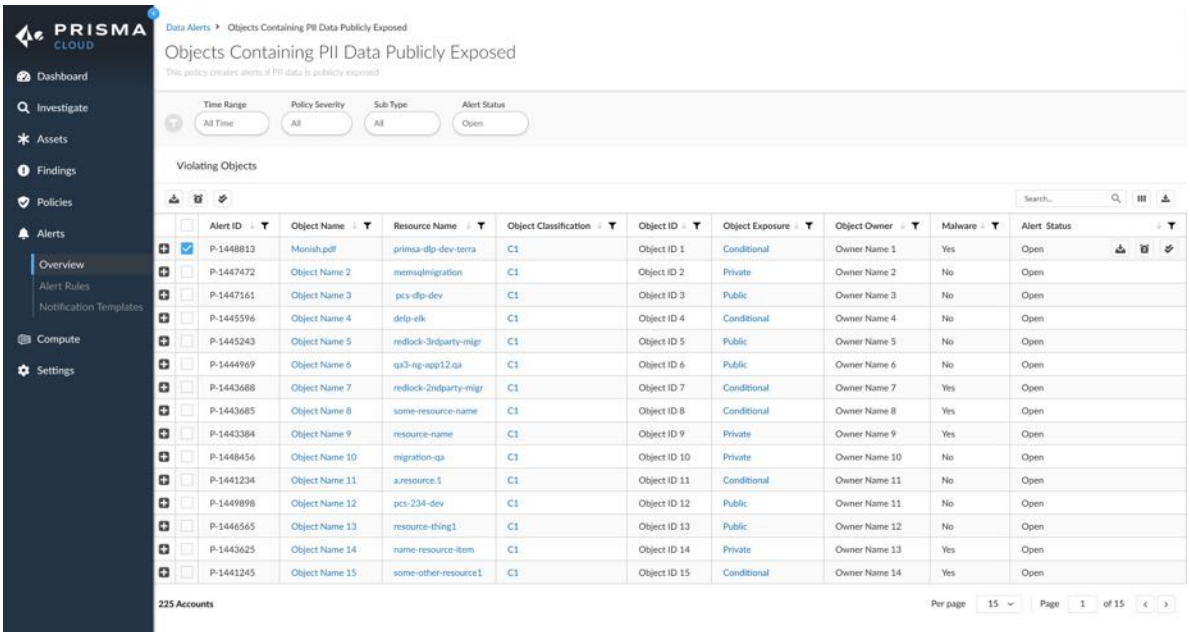

圖 8：PII 的物件掃描結果

「身為主管，我知道自己擁有可以持續監控的工具，晚上就安枕無憂。我的團隊相當投入，我們每天都有人關注 Prisma Cloud。這從此改變了我們維護合規性和可視性的方式。」

—John Hluboky，Veradigm Health 資訊安全副總裁

閱讀完整案例研究。

關於 Prisma Cloud

Prisma® Cloud 是一個全方位的雲端原生應用程式保護平台，可在整個開發生命週期以及混合雲端和多雲端環境中，針對應用程式、數據和整個雲端原生技術堆疊，提供業界最廣泛的安全性和合規性涵蓋範圍。整合式方法可消除原生架構帶來的相關安全限制，而不是試圖加以掩蓋，並且打破整個應用程式生命週期中的安全作業隔閡，進而實現 DevSecOps 並且增強回應能力，滿足雲端原生架構不斷變化的安全需求。

若要了解更多資訊，請造訪我們的網站或立即觀看示範。

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號 6F-1

© 2023 Palo Alto Networks, Inc. Palo Alto Networks 和 Palo Alto Networks 標誌是 Palo Alto Networks, Inc. 的註冊商標。您可在以下網址檢視我們的商標清單：https://www.paloaltonetworks.com/company/trademarks.html。
本文提及的所有其他標誌皆為其各自公司所擁有之商標。prisma_ds_cloud-security-posture-management_040423