

CORTEX DATA LAKE

實現基於 AI 的網路安全創新

優勢

- 收集、整合及規範化企業的安全數據。
- 運用雲端規模數據與計算，套用進階 AI 和機器學習。
- 不斷從新數據來源學習，以發展您的防禦。

辨識及阻止精密攻擊需要針對企業的所有數據使用進階人工智慧 (AI) 和機器學習。目前的方法會使數據隱藏在安全基礎設施的孤島中，限制了分析的有效性。隨著數據持續增加，傳統硬體式部署無法擴充，這會造成營運負擔和高成本；這些傳統部署的容量有限，導致有用的數據難以處理或無法使用。

Cortex 的一部分

Cortex™ 是業界唯一基於 AI 的開放式、整合式的持續性安全平台。藉助自動化和前所未有的準確性，大幅簡化操作並顯著改善安全性成果。

Cortex Data Lake

Cortex Data Lake 採用業界唯一可將您的企業數據規範化並加以整合的方法，實現基於 AI 的網路安全創新。獲取公有雲的規模和位置，同時確保數據的安全性與隱私權。使用上千億個多來源構件進行分析，顯著改善安全性成果的準確性。Cortex Data Lake 可以：

- 透過收集、整合及規範化企業安全數據，從根本上簡化您的安全作業。
- 運用雲端規模數據與計算，輕鬆執行進階 AI 和機器學習。
- 不斷從新數據來源學習，以發展您的防禦。

永遠不用再擔心複雜度或擴大規模問題

部署大量數據收集、儲存和分析基礎設施是很複雜的難題。您必須對空間、電力、計算、網路和高可用性需求、不斷增加的成本以及營運負擔進行規劃。部署完成後，基礎設施需要持續的維護和監控，限縮推動業務發展的活動的時間。

Cortex Data Lake 的建立從公有雲規模和位置獲益。雲端服務的規模從一開始就具有彈性，無需本機計算和儲存。隨著需求成長，您只要按一下按鈕即可新增更多容量。公有雲架構可讓您運用全球位置來滿足本機數據存放和隱私權需求。我們會為您處理包括儲存與運算在內的基礎設施，讓您使用在 Cortex 上建立的應用程式專注於解決新的安全挑戰。

使持續擴展的數據一致

組織往往缺乏阻止攻擊所需的可視性。數據通常單獨鎖定在雲端、端點和網路資產中，導致工具無法有效尋找、調查或自動化威脅回應。

Cortex Data Lake 是業界唯一可將您的企業數據規範化並加以整合的方法。它會自動收集、整合及規範化安全基礎設施的數據。有了一致的數據，便可執行進階 AI 和機器學習，使用 Cortex 上建立的應用程式從根本上簡化安全作業。緊密的感測器整合可持續新增新的數據來源與類型，進而發展您的防禦。





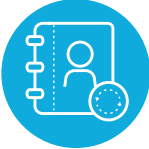
Cortex Data Lake	全球威脅情報
 <p>收集、整合及規範化企業的安全數據，並結合上千億個多來源構件，進行 AI 和機器學習。</p>	 <p>WildFire® 惡意軟體防禦服務會從數萬個獨立組織收集上千億個持續增加的威脅構件。</p>
	 <p>AutoFocus™ 脈絡威脅情報還會使用脈絡與分類 (包括惡意軟體系列、攻擊者、活動、入侵和惡意行為的標籤) 進一步豐富 WildFire 數據。所有構件都會執行統計分析，以判斷其普遍程度與獨特性。</p>
	 <p>MineMeld 威脅情報協調可從任何第三方威脅情報來源進行彙總和指標管理。</p>
	 <p>Directory Sync 提供來自內部部署目錄基礎設施的使用者與群組脈絡。</p>

圖 1：Cortex Data Lake 數據來源

您需要執行的操作	Cortex Data Lake
整合企業的安全數據	收集來自 Cortex XDR、Palo Alto Networks 新世代防火牆、Traps™ management service 和 GlobalProtect™ cloud service 的數據。
擴展您的數據收集需求	受益於公有雲可擴充性和敏捷性，只要按幾下就可以增加容量。您無需等候硬體，只要訂購、啟用、使用即可。
輕鬆存取規範化以進行進階 AI 和機器學習	以一致的格式自動規範化數據，進而確保大規模分析的有效性。
與第三方安全工具整合	可讓您選擇使用 日誌轉送 應用程式，透過系統日誌格式或電子郵件通知，將數據提供給第三方安全工具。

調整部署規模

[使用此計算機](#) 來確定您支援 Cortex 和 Palo Alto Networks 中的創新應用程式與服務所需的儲存空間。

信任與隱私權

Cortex Data Lake 擁有嚴格的隱私權與安全性控制，以防止未經授權存取敏感或可辨識資訊。Cortex Data Lake 透過限制獲得授權的使用者與應用程式的存取權，確保數據的隱私權，您可以隨時撤銷存取權。Cortex Data Lake 基礎設施採用業界標準的安全性和機密性最佳實務進行保護，包括嚴格的技術和組織安全性控制。

Cortex Data Lake 託管於 SOC 2 Type II 合規性數據中心，並在傳輸時對數據進行加密。客戶使用單一登入 (包括雙因素驗證) 來驗證屬於 Cortex Hub 的應用程式。您可在 [我們的隱私權型錄](#) 中找到詳細資訊。

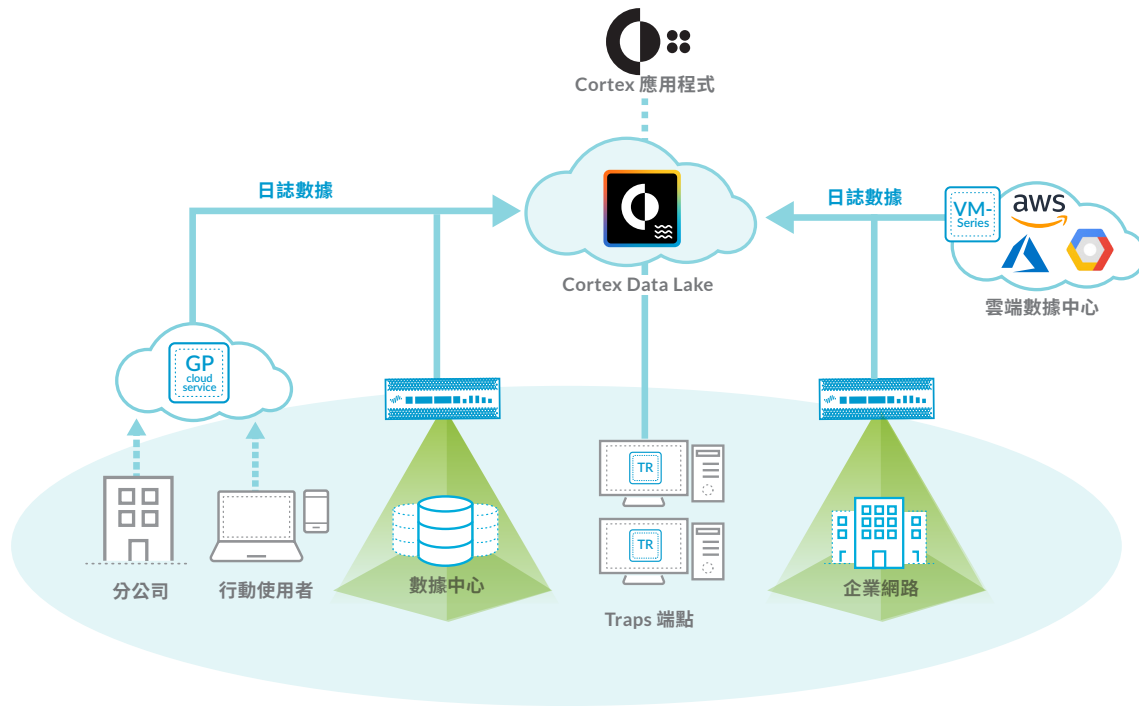


圖 2：Cortex Data Lake 整合

Cortex Data Lake 需求

Palo Alto Networks 新世代防火牆與 GlobalProtect cloud service：

- 新世代防火牆和 Panorama™ 網路安全管理具備連線至雲端服務的能力。
- 新世代防火牆和 Panorama 執行 PAN-OS® 8.0.5 與更新版本。
- Panorama 已安裝雲端服務外掛程式。

Palo Alto Networks Traps™ 端點防護與回應以及 Cortex XDR：

- Palo Alto Networks Traps Advanced Endpoint Protection 執行 Traps management service 5.0 與更新版本。

授權資訊

- Cortex Data Lake 為獨立授權，需要使用 Cortex 與關聯的應用程式。



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 號台北南山廣場 34 樓

© 2019 Palo Alto Networks, Inc. Palo Alto Networks 是 Palo Alto Networks 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。
 cortex data lake-ds-022519