CORTEX DATA LAKE 隱私權

Palo Alto Networks 委託獨立數據隱私權風險管理提供商 TrustArc 審查和記錄本型錄中描述的數據流和做法。本文件的目的是透過詳細說明如何由服務且在服務內擷取、處理和儲存個人資訊，為 Palo Alto Networks 客戶提供評估此服務對其整體隱私狀況的影響所需的資訊。

產品摘要

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。由於此服務的雲端特質，客戶從跨網路的不同位置部署的多個平台產品收集日誌數據，完全不需要規劃運算和儲存。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。

使用 Cortex Data Lake 服務時，客戶不再受硬體可用性的限制，也不再受限於日誌收集器的部署速度。Cortex Data Lake 收集來自 Palo Alto Networks 新世代防火牆、GlobalProtect™ cloud service (將 Security Operating Platform 的保護擴展到遠端網路和行動使用者) 和 Traps™ management service (將平台擴展到執行 Windows®、Linux 或 macOS® 的端點) 的日誌。Panorama™ 網路安全管理透過關聯 Cortex Data Lake 中的可用日誌，提供對整個平台的網路和事件的可視性。

由 Cortex Data Lake 處理的資訊

Cortex Data Lake 從我們業界領先的 Security Operating Platform 接收日誌。任何平台元素發生基於客戶安全政策的相關事件時，將產生日誌以啟用偵測、調查和分析。

來自新世代防火牆的日誌

新世代防火牆將日誌傳送到位於客戶選擇的任何地區的數據中心。客戶可以選擇下列任何類型的日誌傳送到 Cortex Data Lake：

- **流量日誌** - 與來自裝置和使用者 IP 位址的內部和外部網路連線有關的資訊。
- **威脅和 URL Filtering 日誌** - 已知和未知威脅以及防火牆偵測到的網路流量相關資訊。
- **User-ID 日誌** - 網路和應用程式流量日誌相對應的其他使用者和群組對應。
- **HIP 比對日誌** - 已登入 GlobalProtect 的端點相關資訊。只有在連線裝置與設定的資產政策相符時 (例如主機未安裝防毒軟體時)，才會記錄主機資訊設定檔數據。
- **設定日誌** - 對新世代防火牆所做的設定變更 (例如使用者新增安全規則) 相關資訊。

- **系統日誌** - 新世代防火牆作業相關的資訊，例如授權到期。
- **驗證日誌** - 最終使用者嘗試存取由驗證政策規則控制的網路資源時發生的驗證事件相關資訊。
- **GTP 日誌** - 行動裝置通過行動網路時的連線相關資訊。一些行動服務供應商使用 GPRS 通道通訊協定數據為行動裝置建立安全政策。
- **通道檢查日誌** - 追蹤經過檢查的通道工作階段的開始和結束項目。有時會使用這些資訊將政策套用於通道流量。
- **增強的應用程式日誌** - 執行分析所需的資訊，例如 MAC 位址、主機名稱和 DNS 查詢/回應。MAC 位址和主機名稱用於唯一識別網路上的裝置及其模式，而 DNS 查詢/回應用於偵測進階惡意軟體導致的傳出通訊。

上述新世代防火牆日誌中的某些數據可能會被考慮或包含個人資訊。下表詳細列出日誌中包含的資訊類別。

類別	傳送到 Cortex Data Lake 的資訊	範例	可能會被考慮或包含個人資訊
使用者資訊	網域和使用者名稱 使用者名稱	company\john.smith jsmith	是
	電子郵件地址	username1@company.com	是
裝置資訊	MAC 位址	ec-68-81 -22-cc-33 或 00-1b-17-44-55-66	是
	主機名稱	WIN10-JSMITH	是
	國際行動訂戶識別 (IMSI)	410072821393853 460001357924680	是
	國際行動設備識別 (IMEI)	990000862471854 351756051523999	是
	URL 或 DNS 請求中的合格主機名稱	server.company.com	是
	MAC 位址	aa-11-bb-22-cc-33 或 11-22-33-44-55-66	是
	主機名稱	Marys-Macbook.company.com 或 WIN10-JSMITH	是
	作業系統	Macintosh 或 Mac HIP Apple Windows Android	否
	防火牆名稱	NA 防火牆或 DC1 防火牆	否
	防火牆設定使用的其他名稱	vsys1 或信任區域或不信任區域	否
網路位址	來源裝置的 IP 位址	10.10.10.1	是
	目的地裝置的 IP 位址	192.168.10.1	是
其他資訊	PCAP	在防火牆上建立網路流量的封包擷取，並在下列條件下傳送：未知的 UDP/TCP 工作階段。	是
	URL	https://www.linkedin.com/in/jsmith/ https://outlook.office365.com/EWS/Exchange.asmx https://mg.mail.yahoo.com/neo/m/launch?&filterBy=&fid=Inbox&fidx=1&ac=DSTVMBzTbaVaamXPZAndcVWZ22g-	是
	檔案名稱	Financial_report.xlsx John_smith_bio.pdf Corporate_presentation.pptx	是

圖 1：日誌中包含的資訊

記錄欄位名稱	流量日誌	威脅日誌	URL Filtering 日誌	User-ID 日誌	HP 比對日誌	GTP 日誌	通道檢查日誌	驗證日誌	設定記錄	系統日誌	相關聯的事件日誌	增強的應用程式日誌
裝置名稱 (防火牆)	X	X	X	X	X	X	X	X	X	X	X	
來源 IP 或來源位址	X	X	X	X	X		X	X	X	X	**X**	X
目的地 IP	X	X	X				X					X
來源使用者	X	X	X	X	X	X	X	X	X	X	**X**	
目的地使用者	X	X	X			X	X					
寄件者 (電子郵件地址)		X										
收件者 (電子郵件地址)		X										
NAT 來源	X	X	X				X					
NAT 目的地	X	X	X				X					
來源區域	X	X	X				X					
目的地區域	X	X	X				X					
通道 ID/IMSI (*)	X	X	X			X	X					
監控標籤/IMEI (*)	X	X	X			X	X					
MSISDN						X	X					
URL/檔案名稱		X	X								**X**	
數據來源名稱				X								
使用者								X				
Normalize_user								X				
File_url		X										
End_ip_addr						X	X					
Area_code						X						
Cell_id						X	X					X
電腦名稱					X							x
X-Forwarded-For (xff)		X	X									
描述										X		
管理員									X	X		
IPv6 系統位址	X	X	X	X	X		X	X	X	X	**X**	

** 啟用 GTP 模式*

圖 2：按日誌類型區分的個人資訊[1]

來自 Traps Management Service 的日誌

Traps Management Service 從 Traps 端點將資訊轉送到位於客戶選擇的區域數據中心內的 Cortex Data Lake。Traps Management Service 程序的資訊可以分為下列日誌類別：

- **威脅日誌**包含 Traps 記錄的所有安全事件相關資訊，包括惡意軟體和入侵防禦、偵測後事件和限制通知。
- **設定日誌**是 Traps Management Service 記錄的稽核日誌。包括政策事件，例如對 Traps 安全政策、例外管理和設定檔管理的變更。稽核日誌也包括其他設定變更，例如裝置管理、散佈管理和系統管理。
- **系統日誌**包含持續監控 Traps Management Service 和代理程式事件相關的數據。這包括授權管理、代理程式註冊、使用者驗證、代理程式連線狀態、代理程式升級和代理程式保護狀態的變更或更新。系統日誌通常用於日常作業以及支援和故障排除活動。
- **分析日誌** (每小時雜湊執行) 來自每個 Traps 代理程式。這些日誌為追蹤受保護環境中嘗試進行的惡意軟體執行、雜湊例外狀況政策變更和鑑識提供了可視性檔案分析報告佔用大量的 Traps 儲存空間。

Traps Management Service 日誌中的某些數據可能會被考慮或包含個人資訊。如需日誌和欄位的更多細節，請參閱 Traps Management Service 隱私權型錄。

1. 如需每個欄位的詳細資訊，請參閱本文件的「資源」部分。

Cortex Data Lake 如何符合歐盟數據保護法

處理個人數據以確保網路和資訊安全 (包括透過雲端數據處理器)，被公認為「合法權益」，且特別以下方文字列於歐盟一般數據保護法規：

> *(49) 為確保網路與資訊安全而嚴格遵循必要性及合比例性之個人數據處理 (亦即，具有指定機密級別之網路或資訊系統，以防止突發事件或違法或惡意行為危害已儲存或已傳輸之個人數據之可用性、真實性、完整性及機密性，及危害藉由該等網路或系統、公務機關、資安危機應變小組 (CERT)、資安事件處理小組 (CSIRT)、電子通訊網路及服務供應商及安全技術服務供應商所提供相關服務之安全性)，構成相關數據控管者之正當利益。*
>
> *例如，這可能包括防止未經授權而存取電子通訊網路和惡意程式碼散佈，並阻止「阻斷服務」攻擊以及對電腦和電子通訊系統造成損害。*[2]

Palo Alto Networks 等服務供應商處理個人數據以確保網路和資訊安全，這是服務供應商及其客戶的合法權益。這種合法權益為 Palo Alto Networks 根據歐盟數據保護法處理個人數據提供基礎。這種合法權益通常也為根據隱私權或可阻止客戶共享特定數據的法規要求在 Cortex Data Lake 中儲存個人數據的客戶提供基礎。在這種事件中，客戶可以使用自己的隱私權選項，如本文所述，在設定防火牆或 Panorama 管理帳戶時限制數據處理或數據存取。

Palo Alto Networks 如何遵守數據保護規則

Palo Alto Networks 致力於保護 Cortex Data Lake 中儲存和處理的個人數據。除非在解決平台或 Cortex Data Lake 問題時有必要，否則我們不會為了瞭解有關自然人的有意義資訊，以這種方式存取資訊。

原始日誌的處理自動化進行，並且日誌將保留，直到根據客戶可用的儲存量或客戶套用的保留政策覆寫日誌為止。此外，絕對不會與任何第三方共享這些資訊。

Palo Alto Networks 系統儲存或處理的任何日誌均採用最先進的技術予以保護，並且 Palo Alto Networks 採用嚴格的技術和組織安全性控制。轉送到歐洲數據中心的日誌和資訊將保留在歐盟境內。由於 Palo Alto Networks 是一家跨國公司，在某些情況下可能需要與其他地區的 Palo Alto Networks 公司共享日誌和資訊。我們只會按照歐盟數據保護法中所述，根據歐盟委員會或其他法律機構基於個人數據傳輸所核准的歐盟標準合約條款來共享資訊。

客戶隱私權選項

客戶可以根據自己的政策啟用或停用與 Cortex Data Lake 共用日誌類型。但是，無法自訂日誌類型內容和日誌數據屬性。客戶也可以透過 Panorama 控制對 Cortex Data Lake 中的資訊進行的存取。此外，客戶可以選擇特定的區域數據中心來儲存日誌。

存取和揭露

客戶存取

客戶可以透過 Panorama 存取自己的防火牆和 GlobalProtect cloud service 日誌，並在需要時匯出特定鑑識的日誌子集。對於 Traps Management Service，客戶可以透過 Traps Management Service 使用者介面存取日誌。

若啟用，將收集增強的應用程式日誌。可以對這些日誌處理，以提供異常網路活動與始發裝置和網路介面 (例如 Wi-Fi 或乙太網路介面卡) 的關聯和歸因。可以透過處理應用程式的介面查看已處理日誌的結果。

Palo Alto Networks 存取

支援案例開啟時，僅限 DevOps、數據中心、威脅研究和分析團隊以及客戶支援團隊可存取 Cortex Data Lake 中的原始日誌。允許為了進行疑難排解、解決問題以及提高安全保護的有效性而存取。

保留

Cortex Data Lake 允許客戶根據其保留排程或儲存大小設定保留期間。例如，保留期間設定為三十天，日誌將在收到後的第三十一天刪除。如果將保留大小設定為 100 TB，在達到儲存容量之前不會刪除日誌，這表示保留期間將取決於傳入日誌速率。

在 Cortex Data Lake 終止後，系統將在三十天後清除數據。

2. GDPR，陳述 49；另參閱 2014 年 4 月 9 日通過關於數據控制器合法權益概念的第 29 條工作組意見 06/2014，第 24-25 頁。

Cortex Data Lake 的日誌數據安全性

傳送到 Cortex Data Lake 的日誌在傳輸到客戶選擇的數據中心時被加密。Cortex Data Lake 使用的數據中心採用最先進的實體和網路安全措施進行防禦和保護，後者由我們業界領先的 Security Operating Platform 提供。Palo Alto Networks 同樣通過了 Cortex Data Lake 的 SOC 2 Type II 認證，這展示其本身強大的安全政策和內部控制環境。此外，該服務由 SOC 2 Type II 認證數據中心託管。

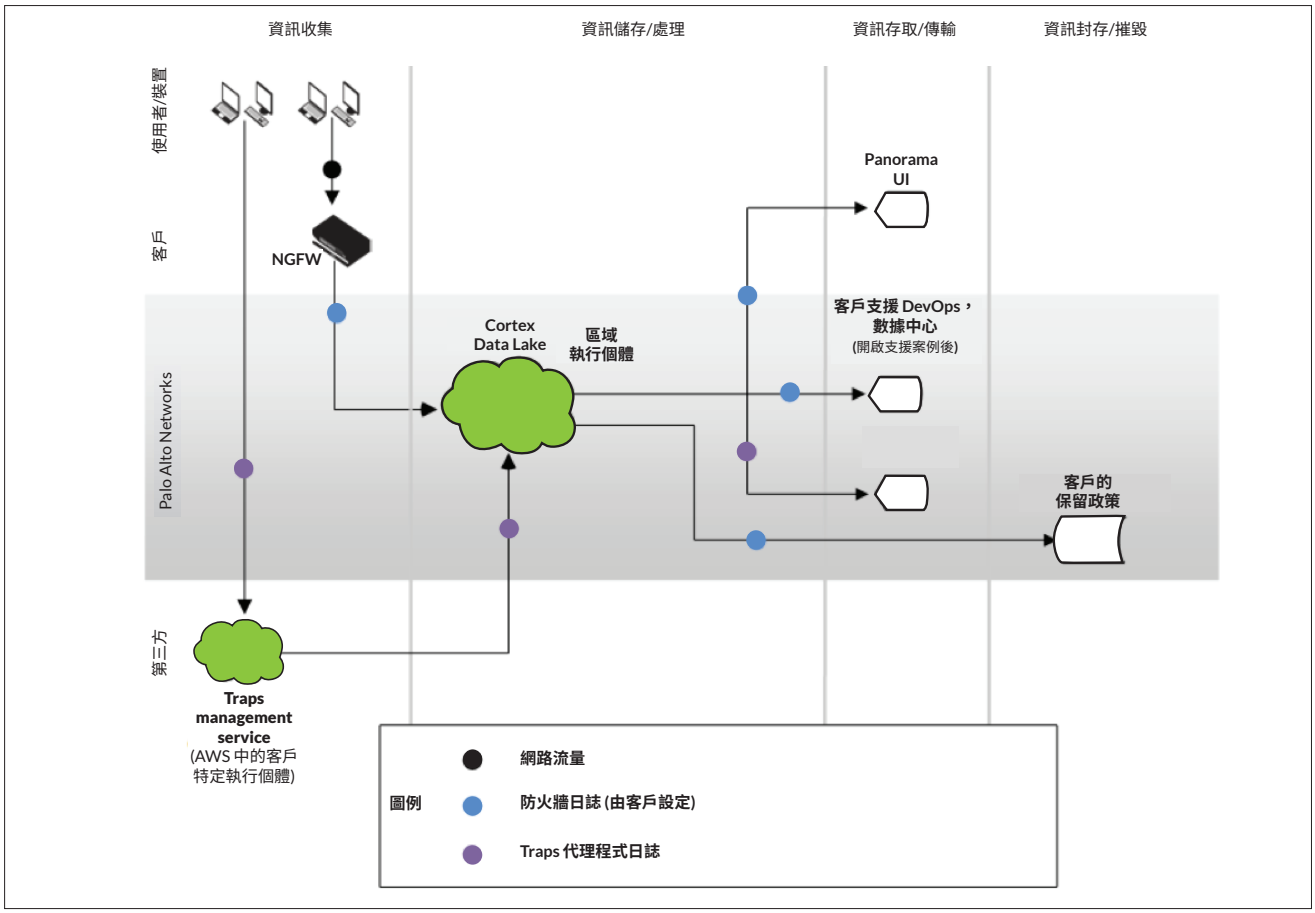

圖 3：數據流程圖

資源

如需 Cortex Data Lake 和相關 Palo Alto Networks 服務的詳細資訊，請參閱下列資源：

- Cortex Data Lake
- Panorama
- Cortex
- Traps management service
- Cortex XDR
- Security Operating Platform

關於本型錄

本文包含的資訊依據文件審查以及與所述服務開發和營運相關的主題專家訪談。發現過程仰賴所提供資訊的誠信準確性；TrustArc 尚未進行獨立稽核，也未對本型錄中包含的資訊進行認證。但是，截至本型錄首次發佈時，本文包含的資訊據信準確且完整。請注意，本文提供的技術或專業主題相關的資訊僅供一般參考，可能會有所變更，並不構成法律或專業建議，也不保證適用於特定目的或遵從適用法律。

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

cortex-data-lake-privacy-ds-022519