透過 Palo Alto Networks 解決雲端安全挑戰

不斷加快的雲端移轉

雲端運算無處不在：根據 2022 年的 IDC 報告，全球有超過 90% 的企業將依賴混合的內部部署或專用的私有雲、多個公有雲以及舊型平台以符合基礎結構需求。[1]

由於雲端運算無處不在的特性，它已逐漸成為網路攻擊的主要目標。移轉至雲端可協助簡化及提升某些層面的安全性，例如，基礎結構層。

不過，雲端部署也已對安全性構成新的挑戰，而許多企業都不常處理這些問題，甚至不知道如何更有效率地加以因應。在嘗試解決雲端安全問題時，許多企業都發現他們並無法輕易地將內部部署方法直接轉換至雲端。

1. 「IDC Expects 2021 to Be the Year of Multi-Cloud as Global COVID-19 Pandemic Reaffirms Critical Need for Business Agility」，IDC，2021 年 3 月 30 日，https://www.idc.com/getdoc.jsp?containerId=prMETA46165020。

雲端安全中的許多角色

雲端安全性包含了各種不同類型的活動，例如設定管理 (從安全角度而言確保雲端資產的設定正確無誤) 以及深入的調查和回應 (處理在企業環境中的任何地點偵測到的威脅，並尋找與該威脅相關聯的惡意活動)。

視企業而定，這些活動都是分屬於與雲端安全性有關的許多不同角色和團隊功能：

- 雲端基礎結構工程師和架構師
- 安全架構師和工程師
- DevOps 與 DevSecOps 團隊
- 監管、風險與合規性 (GRC) 團隊
- SOC 經理
- 安全分析師、事件回應者和威脅捕捉專家
- CISO

同樣地，視雲端計劃的執行和組織方式而定，每個團隊相對於其擁有權都會有不同的需求。此外，視計劃而定，某些團隊的擁有權範圍也各自不同，有的較寬、有的較窄。

表 1：雲端安全性的角色和責任

團隊/角色	關鍵責任
雲端基礎結構工程師和架構師	設計雲端環境；雲端和容器平台的部署及整體擁有權
安全架構師和工程師	同時涵蓋雲端和 SOC 團隊；實作公有雲環境和新型雲端原生架構 (例如雲端虛擬機器、容器、Kubernetes 和無伺服器) 的安全性
DevOps 與 DevSecOps 團隊	管理雲端基礎結構部署；設計大規模的雲端原生架構
GRC 團隊	針對業務的風險進行監控及通訊
SOC 經理	確保安全作業能跟得上業務的速度；降低停留時間
安全分析師、事件回應者和威脅捕捉專家	監控、偵測、調查和回應橫跨雲端和內部部署的威脅
CISO	整體雲端進程和投資的安全性

雲端安全挑戰

雲端安全挑戰會因為每個團隊所負責解決的挑戰不一而有所不同。一般來說，這些都是雲端原生環境以及混合雲/多雲端環境所特定的需求。

大部分的安全團隊都與 DevOps 一樣抱持著「越快移轉越好」的心態。他們的責任是保護那些與建置到執行之程序直接連結的雲端原生應用程式。他們的挑戰是確保這些應用程式在持續不斷及快速重複的建置至執行週期期間或之後，不會成為各種威脅和安全問題的犧牲者，其中包括：

- **應用程式中的弱點：**應用程式的程式碼若未透過正確的工具進行掃描，可能會將已知的 CVE 導入至最為關鍵的環境中而遭到攻擊者入侵。而對於許多不同的環境和應用程式生命週期來說，要解決這些問題則會面對更大的挑戰。
- **不安全的設定**：一旦發生設定錯誤，無論是應用程式本身或其執行的基礎結構出錯，都會增加風險。例如，像是錯誤設定的儲存空間陣列、不安全的網路設定或是以根身分執行的應用程式，都會增加企業的整體風險。
- **缺乏執行階段保護：**若對於檔案系統活動、網路通訊、程序活動和系統叫用活動缺乏適當的可視性和保護，則在執行應用程式時將很容易遭到攻擊。如果沒有正確的安全解決方案，企業將會因為無法預防威脅或取得鑑識活動以進行深入事件分析而暴露在風險中。

- **對於網路通訊的可視性和控制：**微服務和應用程式工作負載能夠互相通訊以及與外界進行通訊。安全和基礎結構團隊必須了解應用程式相依性、縮小其雲端網路威脅面並遏止任何網路攻擊。
- **公有雲上過度授予的權限：**由於企業會雇用大量的開發人員、DevOps 工程師、平台工程師和其他重要的利益關係人，因此他們必須確保每一位使用者都具有適當的雲端權限。然而，包括為每個使用者進行手動設定、不具備自動稽核雲端權限的能力，以及缺乏正確設定的權限都會對單一和多雲端環境持續形成挑戰。

安全營運團隊會負責維持雲端應用程式開發以及生產部署的正常運作，並確保雲端環境都具備適當的工作流程以進行威脅偵測、調查和回應。他們的挑戰是必須能夠同時檢視內部部署和雲端環境，此外不單只是具備可視性，還必須充分利用可視性而不能套用新的方法或將內部部署方法轉換至雲端。他們的核心挑戰如下：

- **偵測擴散至整個企業的威脅：**威脅偵測機制並無法讓您能夠輕鬆地收集、處理及分析雲端數據以及內部部署環境和資產。
- **簡化雲端環境中的事件回應：**安全營運團隊經常需要在內部部署活動與雲端活動之間切換脈絡，因為他們通常會透過不同的工具存取，或者是使用個別或不相關的工作流程來分類警示、執行臨時操作分析，或進行威脅的深入調查以界定範圍或執行鑑識分析。
- **在多個數據來源之間建立威脅活動的關聯性：**對於維護數據收集內部部署的營運團隊來說，實際上他們並無法將雲端數據傳送至集中記錄平台來執行跨數據分析。對於雲端託管的數據記錄來說，將雲端、端點、網路和使用者數據的深入脈絡集中至單一位置不但非常昂貴，並且/或者會構成技術上的挑戰 (或不可行)，且用來偵測威脅的分析技術並不具備必要的整合深度以正確脈絡化各種事件，因此無法處理這些數據來源。
- **取得橫跨雲端和內部部署的威脅導向脈絡：**事件回應團隊必須能夠隨時從威脅警示、事件、資產、威脅情報和所有第三方數據來源 (包括雲端和內部部署) 取得完整的威脅脈絡，以便他們執行完整的調查以取得確實可行的結果。
- **不同的雲端警示使警示麻痺更為惡化：**監控和分類團隊無法輕鬆地將可疑雲端活動整合至更為廣泛且已充斥各種雜訊的警示佇列，造成驗證不足的情況加劇、對於因果關係缺乏了解或過於膚淺、無法輕鬆地建立事件時間表，以及整體程序片段化的情況更為普遍。

一般來說，雲端原生安全團隊與更為傳統的 SOC 團隊對於安全性、使用者體驗、調查方法和回應工作流程的需求大不相同。

其中最主要的原因就是雲端安全團隊能更確實地反映雲端應用程式開發和部署的建置至執行週期程序，首先會需要：

- 雲端安全性基礎層面的深度和廣度
- 盡可能地涵蓋最大範圍的雲端活動
- 對於雲端環境最深入的見解

然而 SOC 團隊通常皆已具備現有的程序並著重於：

- 整合整個企業的觀點以取得關鍵的調查脈絡以及必要的正確遙測以進行威脅偵測和分析
- 確保雲端脈絡會更深入地整合，針對整個企業取得對於威脅活動的全貌

透過 Palo Alto Networks 取得全面的雲端安全性

現今大部分的企業都會使用舊型 SOC 工具的組合 (例如 SIEM 加上 CSPM 或 CWPP 解決方案) 來解決這些挑戰的特定層面。這個方法的最大問題就是它無法以原生方式整合端點、網路、雲端和身分數據，在更廣泛的混合環境中脈絡化各種雲端威脅。

另一個方法就是評估作為雲端安全性工具上市的 EDR 或 XDR，以嘗試解決整個點對點問題。此一方法的主要挑戰就是 EDR/XDR 其實是一種 SOC 最佳化的工具，且不符合雲端安全團隊的獨特安全性、可用性和速度等需求。

Palo Alto Networks 會提供獨特的雲端安全解決方案，以同時符合雲端安全性和傳統 SOC 團隊的深度、涵蓋範圍和營運需求。

Prisma® Cloud 會提供完整的生命週期弱點管理、合規性監控和執行階段保護，使雲端安全團隊可針對雲端中執行的應用程式排定優先順序並降低風險。Prisma Cloud 也會確保雲端資源和環境的安全設定、識別公有雲上過度授與的權限，並結合網路可視性和微區隔以提供全面的雲端網路安全性。

Cortex® XDR™ 可為 SOC 團隊提供雲端功能，使其能著重於整個企業的威脅監控。Cortex XDR 能提供 SOC 團隊所需的雲端功能以擴大其對於雲端環境的偵測、監控及調查範圍。XDR 會將雲端主機數據、流量日誌、稽核日誌、Prisma Cloud 數據和第三方雲端安全數據與非雲端端點、網路和身分數據來源進行整合，使 SOC 團隊能增加對於跨內部部署和多雲端環境的涵蓋範圍。

表 2：Prisma Cloud 和 XDR 的雲端功能

功能	Prisma Cloud	XDR 中的雲端功能
執行階段安全性	應用程式控制並允許自動列出設定檔主機和應用程式行為對下列各項發出警示或阻止惡意的程序和網路行為：檔案完整性監控；數據摘要提供弱點、可疑的 IP 清單、反惡意軟體和進階威脅防護數據；OWASP 前 10 大威脅防護；DOS 防禦；Bot 防護和虛擬修補	Linux 主機 EDR 提供行為威脅防護、暴力破解法防護、核心完整性監控、檔案/dll/巨集的本機分析、權限提升防護、shellcode 防護和共用物件劫持防護
分析技術	針對雲端應用程式、主機、Kubernetes 和無伺服器進行分析以識別威脅來源 (例如弱點、映像、設定和變更者)，並進行網路和使用者行為分析以偵測異常活動	跨數據分析涵蓋了端點、網路、身分和雲端以自動建立關聯性，並結合偵測和回應功能以識別與事件有關的所有證據和惡意活動
事件管理	專為雲端和 DevSecOps 團隊所設計以識別任何威脅，並針對弱點、設定、權限以及應用程式和資源的可疑活動進行鑑識，同時針對這些資源提供活動歷史記錄	專為 SOC 分析人員所設計，可透過自動化及臨時關聯性收集證據和額外脈絡以找出與警示有關的所有惡意活動，藉此調查該威脅的影響
威脅偵測	Prisma Cloud 機器學習式偵測器會針對公有雲、主機中的網路流量日誌、稽核日誌和雲端資源以及公有雲和內部部署中的應用程式自動擷取數據	XDR 機器學習式偵測器會在端點、網路和身分數據來源中自動建立各結果之間的關聯性
透過警示分組、因果關係和時間表實現事件建立自動化	透過建立設定數據與使用者行為和網路流量之間的關聯性，警示會顯示錯誤設定和威脅脈絡；並以視覺化方式調查雲端數據外洩、雲端帳戶入侵、雲端政策違規以及不符合產業基準的情況	著重於透過自動化方式進行警示、脈絡和威脅數據的整合，以針對需要在內部部署和多雲端環境中監看企業內所有相關威脅活動範圍的事件回應者，提供點對點的事件歷史記錄

Prisma Cloud 與 XDR 雲端功能的結合將可提供現今最為全面的雲端安全解決方案，啟用從建置、執行到安全作業的完整雲端安全性。

請造訪我們的網站，深入了解 Prisma Cloud 和 Cortex XDR，或參考下列資源：

- Prisma Cloud 技術簡介
- Prisma Cloud 產品文件
- Cortex XDR 產品文件
- 新世代已經到來：第三代 XDR 發佈

paloalto NETWORKS | Cybersecurity Partner of Choice

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