買家指南

想找出最符合需求的安全平台嗎?

提出合適的問題，就能得到準確的答案。

IBM Security

IBM

選擇正確的安全平台

為自家企業組織尋找安全平台或許是項艱鉅的任務。在網路安全的領域，「平台」一詞已經被過度使用，導致企業難以消除「雜訊」，也難以瞭解哪些才是企業在決定最佳業務選項的首要考慮的因素。您今天所選的平台將會奠定接下來幾年間安全成熟度的基礎，因此應謹慎選擇。

企業安全團隊面臨資料和工具過多以及資源不足的挑戰。就現況來說，我們需要採用另一種方式來統一管理安全資料、工具和團隊，將所有內容集中儲存也是迫在眉睫的需求，而這便是整合式安全平台的優異之處。

您希望安全平台具備的功能

要尋找可以在此刻和未來均能高效運作的全面整合式網路安全平台，以下因素必須納入考量：

- 與資料轉移相關的考慮事項
- 部署選項
- 您需要串連的其他工具
- 平台的開放性與適應性
- 支援的功能和服務

請考慮以下關鍵問題，有助於瞭解採用安全平台時的選項，並確定哪個選項最適合您的企業組織。

1 您是否需要轉移資料並從中擷取價值？

許多安全平台需要將所有資料轉移到平台上才能存取這些資料。雖然將所有資料儲放在單一位置似乎是個好辦法，但也可能會很複雜且成本高昂。此外，這也可能代表必須著手解決重要的隱私和資料留存問題。

以成本和複雜度的面向來分析，如果平台能連接到存放資料的位置，而無需移動資料，絕對是有益。這種方法可以補足現有工具之不足，最大化投資報酬率，同時亦可提供集中式檢視圖，並存取已分散在各種工具中的資料。

2 您是否可在系統內部、公有雲或私有雲進行平台部署？

許多安全平台僅以軟體即服務 (SaaS) 的雲端解決方案提供。雖然這項做法正確，但許多企業組織尚未準備好只用雲端解決方案，因此需要借助混合多雲架構的靈活性。由於許多企業組織的工作負載仍在內部，因此可靈活地在內部、公有雲或私有雲中執行的安全平台，相對來說比較合適。與其拘泥於單一部署選項，倒不如尋找可以在混合、多雲環境中部署的靈活架構。

3 該平台是否支援串連合作廠商的工具和整合？

如今，企業組織使用的安全工具五花八門，不太可能全部來自同一個供應商。某些安全平台僅適用於整合特定供應商的工具，因此可能處處受限。如果您使用眾多不同供應商推出的安全工具，就需要尋找可支援一系列安全工具和 IT 工具，並進行開放串連的平台。您尋找的平台需要包含以下內容：

– 龐大的合作夥伴生態系統

– 開放式軟體開發組件 (SDK)

– 用於新增自訂連接的支援服務

這種方法有助於確認平台是否能與您的工具相容協作，亦可減少翻新和取代現有工具的需求。

4 當您的安全計畫有異動調整，平台是否能夠進行相應調整？

選擇平台時，最重要的是要考慮平台是否具有足夠的開放性和靈活性，才能為您的安全計畫提供支援。考慮平台是否能夠提供：

– 開放標準

– 開源技術

– 開放連接

開放平台能夠串連合作廠商的工具，而且支援客製化連接和開發。這種方法有助於降低被供應商套牢的機會，並且能夠與多種安全工具和 IT 工具的相容互通。

5 是否能夠提供核心編排、自動化和回應功能？

安全編排、自動化和回應 (SOAR) 解決方案通常被定位為平台本身。不過，將 SOAR 功能內建到主要的安全平台後，這些功能會變得更強大，而不是單獨個別提供。因此，您需要尋找一個以 SOAR 作為核心功能的安全平台，協助提高安全團隊在一系列工作流程和安全案例中的效率。

6 如何支援整合安全威脅的情報？

安全分析師經常使用各種威脅來源和不同的產品來整理過濾威脅情報，做為研究和決策的依據。因此應考慮安全平台能否提供威脅情報報告，以及這些情報如何與其他功能相整合。將威脅情報整合到安全平台中，安全分析師不僅可減少工作量，還能更迅速、更明智地做出決策。

7 供應商是否能夠提供軟體以外的服務？

雖然安全平台已經是功能強大的工具，但您或許會發現還需要其他企業組織或安全計畫專用的服務。安全服務的選項眾多，但如果先從具備安全服務的供應商中做選擇，那麼新增服務，將服務與您的安全平台相整合，便能更簡單輕鬆。

瞭解您安全平台的核心需求

平台的導入可以成為簡化安全資料、工具和團隊的方式。不過，由於選項眾多，因此在替自家企業評估安全平台時，最重要的是要找出以下這些關鍵問題的答案：

– 您是否能將資料保留在原位？

– 您的部署是否支援多雲混合架構？

– 您是否需要開放式整合，串連其他安全或 IT 工具？

– 您是否可以輕鬆因應安全計畫的異動，進行調整？

– 您是否能獲益於安全編排、自動化和應變功能？

– 如何整合威脅情報？

– 您的供應商是否能提供軟體之外的安全服務？

IBM Cloud Pak for Security：專為混合式多雲世界而建構的網路安全解決方案

IBM® Cloud Pak™ for Security 是一個開放的整合式安全平台，具備深入洞察力，掌握目前及未來的跨環境威脅。您可以搜尋威脅、編排行動並自動執行回應，而無需遷移資料。

藉著開放標準和 IBM 的創新成果，IBM Cloud Pak for Security 讓您能夠存取 IBM 和合作廠商的工具，以及跨雲端或內部搜尋威脅指示器。IBM 透過 OASIS 開放網路安全聯盟提供 IBM Cloud Pak for Security 中所用的開源程式碼技術，並與數十家公司攜手合作，以互通有無，並降低被供應商套牢的情況。

IBM Cloud Pak for Security 與 RedHat® OpenShift® 企業應用平台預先整合了容器化軟體組成。透過這種整合，可以在內部及私有雲或公有雲中執行。借助內含的 SOAR 功能，IBM Cloud Pak for Security 可幫助您實現安全回應的編排和自動化。

想瞭解更多 IBM Cloud Pak for Security 的相關資訊

請造訪 IBM Cloud Pak for Security 網頁，瞭解如何發現潛在威脅並依據風險程度做出明智的決策，進而對團隊的進度優先排序。

此外，如果您需要其他人才和技能來支援您的團隊，則可以利用 IBM Security 的服務來擬定可靠的戰略並實現安全計畫的轉型。

台灣國際商業機器股份有限公司
台北市 110 松仁路 7 號 3 樓

2020 年 1 月