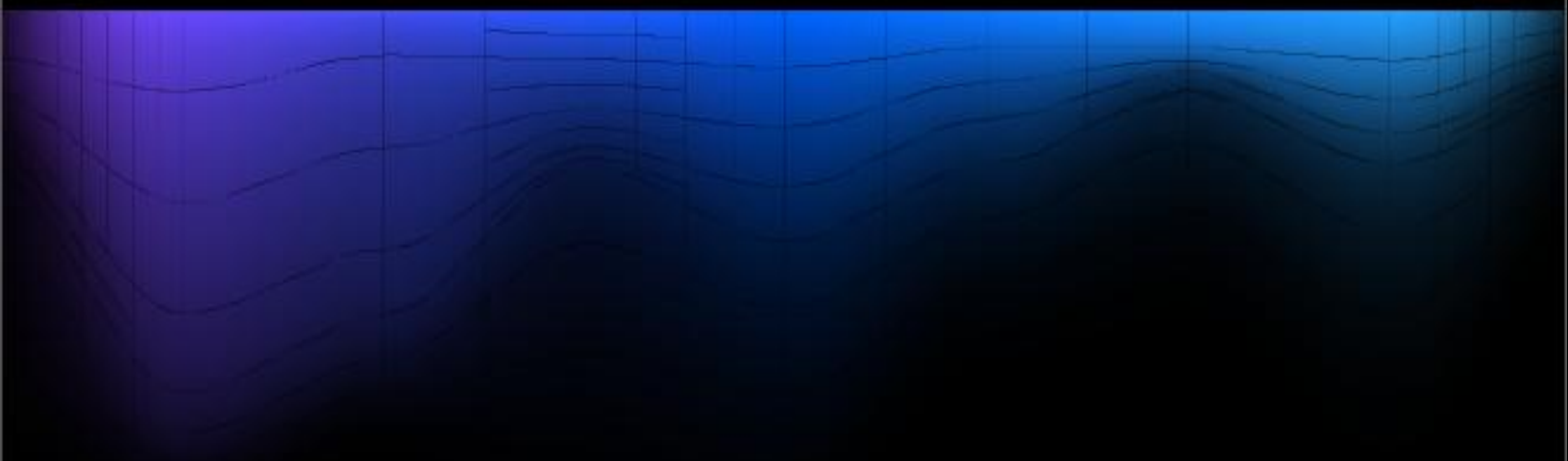
消費者指南

全球資安託管服務供應商：比較

您的供應商是否滿足下列八項標準？什麼樣的資安託管服務供應商（MSSP）是您的首選？回答以下問題以評估您的選擇。



IBM Security

IBM

選擇 MSSP 須考量的八大問題

若要在全球經濟環境中一較高下，企業必須具備快速創新與高效率營運的能力。網路安全工具和服務有助於推動業務發展。MSSP 可以提供專業知識和頂尖技術，並能夠向企業領導階層、利害關係人和客戶證明投資他們是合理的選擇。MSSP 應該滿足 CRO 和 CCO 的風險與合規需求，並落實 CIO 和 CISO 的資安目標。若要尋找能解決這些問題的供應商，請查看下列適用貴公司的八大問題與答案。

1.

MSSP 提供哪些和風險型資安策略直接相關的重要指標？

未分析–僅考量資安事件監控。
（1 分）

不完善的解決方案
這種 MSSP 供應商可以指出企業存在的安全漏洞。除了提供這些資訊以外，這種供應商無法在安全漏洞以及未來風險帶來的潛在可能和影響為您提供任何建議。

有分析，但客戶必須自行釐清資安事件的輕重緩急，並決定要採取的策略與行動。
（2 分）

知識強度不足
隨著資料量增加，您對資料潛在風險評估等級會提高。然而，供應商不會建議您如何解決資安事件問題。

客戶能夠主動防護與應變，管理威脅的同時又能兼顧營利。
（3 分）

完整的服務
這種供應商提供系統管理服務，包含風險、建議、原則與規則。這種 MSSP 可以偵測、應變並回報威脅，若未解決危險，還會提供反映企業成本的資料。

2.

該解決方案與您現有技術投資的整合情形為何？

該解決方案是獨立產品。
（1 分）

有限的功能
MSSP 供應商系統無法與您其他服務或頂尖技術產品連結，因此破壞了這些產品原有的效果。您必須額外採取行動安裝新設備，這會導致您還未開始任何資安工作就已耗盡自身資源。

您可以將其資安託管服務與自身某些技術共同部署。
（2 分）

束拼西湊的合作關係
有了這些解決方案，您可以在一定程度上和 MSSP 共享各種服務或優秀產品。問題在於這類供應商的產品和您的工具可能不相容，導致您需要尋求其他解決方法。

產品管理、開發、資安營運中心和技術之間的合作關係緊密。
（3 分）

可擴展與客製化
這種供應商設計的資安策略可以隨著貴企業的數位轉型或雲端遷移過程來調整。頂尖的 MSSP 供應商秉持產品中立原則，建立良好合作關係，讓他們的工具可以滿足您的需求。

3.

資安事件監控技術有多尖端與面面俱到？

客户只能獲得基本的資安事件監控服務。
（1 分）

一招不能打遍天下
無法提供資安防護層級或附加元件的供應商，可能無法因應貴企業的變化。您將獲得最初階的客戶服務，享有的服務和 MSSP 提供給其他企業的（不論規模和範圍大小）相同。這種 MSSP 訂定一套標準的相關聯規則，並不會依照客戶環境調整，也沒有量身打造的解決方案。

提供幾種選項，但沒有一種選項是全面的解決方案，可以包含發現、監控、建議及防範資安事件和威脅等各層面的作業。
（2 分）

行動有所不足
若供應商沒有靈活的方案來提供全面的資安監控與防護，則企業領導階層很輕易就會找出缺點。若無法為企業量身打造，即使這種 MSSP 提供的是最高階的產品，也無法解決您可能遇到的一些迫切且反覆出現的資安問題。

客戶擁有各式各樣的選項，例如發現、監控、分析，以及包含分散式阻斷服務（DDos）防護、高級威脅情報（暗網監控）以及身份與存取管理等防護。
（3 分）

包山包海的選擇
最完善的 MSSP 提供全面的資安管理與監控，以及威脅情報、事件應變和威脅捕捉等其他功能。他們能夠全年無休全天候快速為您解決問題，並提供一套可以為您量身打造的服務，以滿足您在風險、合規和資安的需求。

4.

供應商是否能為您量身打造適用當地地理環境的服務交付？

未提供客製化服務。
（1 分）

什麼都有或什麼都沒有
有些供應商在全球服務區域交付的資安託管服務相同。這些供應商所供應的服務在客製程度上有限，且並未考量實際企業需求。

僅在已選擇的區域提供當地服務交付。
（2 分）

提供部分協助
這些供應商有會說特定國家主流語言的員工。這樣的安排可以促進互動、提升客戶滿意度，但僅限於有提供服務的這些國家。

兼具在地化與全球規模的供應商。
（3 分）

廣闊的觀點
您希望供應商能夠全方位瞭解您的業務需求。最厲害的 MSSP 會考量您所處的地理環境和全球文化，為您量身打造資安解決方案。這些 MSSP 放眼全球，瞭解各地在監管、資料與隱私等各個面向的要求。

5.

供應商是否可以提供現代數位體驗，並讓您可以一手掌握資安營運中心？

這種供應商不提供任何行動應用程式。
（1 分）

存取延遲
負責讓辦公區遠離資安事件警報的 CISO 或 CIO 所要面對的是運作不善的應變流程。他們得連上筆電、登入 MSSP 入口網站、尋找案例或故障單，這樣的流程有諸多不便之處。

有提供行動應用程式，但載入速度慢，無法提供充分的互動或結果的可見度（或兩者皆無法提供）。
（2 分）

可用性不定
時間是解決資安威脅的關鍵。若一種服務的應用程式阻礙快速行動的能力，缺乏制定決策的所有必要資訊（或兩種情況皆有），則您會發現其功能無法滿足您的需求。

客戶擁有一款全年無休的應用程式，能夠迅速開啟，並清楚顯示所有詳細資訊。
（3 分）

隨時上線提供服務
有了可靠的行動應用程式，無須筆電就能開始作業，快速應變資安事件。拿起手機、開啟應用程式、查看事件的嚴重性、關鍵性和相關背景，然後快速制定決策。

6.

供應商如何應變事件？

事件應變不在 MSSP 的工作範疇。
（1 分）

這項重責大任由您自行承擔
這種供應商基本上只記錄您遇到哪些安全漏洞以及這些漏洞造成的破壞。您必須自行決定如何處理事件，或與其他供應商合作。唯一可以確定的是，這會耗費您額外的時間和資源。

供應商僅提供一種選擇，遠端應變或本機應變。（2 分）

一半的答案
您需要靈活的應變能力。一些複雜的安全事件需要在企業內部搶救。而有些事件則是發生之際便需要立即協助。這種 MSSP 無法充分應變貴企業的需求。

這種供應商既可提供遠端應變，也可以提供本機應變。（3 分）

防護措施準備就緒
這種供應商幾乎能夠抵擋企業面臨的所有資安攻擊，提供檢測與應變管理服務。提供這種附加服務的頂級 MSSP，還會使用系統關鍵性分數來瞭解漏洞事件的背景，以避免類似事件再次發生。

7.

MSSP 能否在混合式多雲環境中提供整合策略與可視性？

供應商僅為本機環境提供服務。
（1 分）

片面洞察
專家一致認為，多數企業的資安監控服務需求範圍也包含雲端交付服務。若供應商無法管理公有雲或私有雲的資安事件，就無法滿足您目前的 IT 資安需求。

MSSP 提供本機服務與基礎架構即服務 (IaaS)
（2 分）

仍存在一些漏洞
由於平台即服務（PaaS）和軟體及服務（SaaS）的使用頻率很高，所以需要採用和 Iaas 相同的安全性標準。例如，這種 MSSP 無法監控或檢測基礎架構或來自第三方大多數應用程式的威脅。

您可以涵蓋各式各樣的混合式多雲環境，包含 IaaS、PaaS 和 SaaS。
（3 分）

為提供雲端服務做好準備
這種 MSSP 擁有專業技術與知識，能夠輕鬆應對所有雲端環境的複雜問題。對於運用微服務和容器化（例如，熱門開源容器應用程式 Red Hat OpenShift）提供原生雲端的現代應用程式，這種供應商可以監控和應變這些應用程式所面臨的各種威脅。

8.

為了檢測事件並釐清事件的輕重緩急，供應商運用機器學習進行資安分析的程度有多高？

未使用機器學習。
（1 分）

跟不上潮流
許多安全檢測裝置現在都使用機器學習來提升交付服務的效率。若供應商提供的服務缺乏這種能力，會造成貴企業需要經常應變類似事件且速度緩慢。這種 MSSP 傳送大量雜訊與低價值資訊讓您處理。

使用機器學習的程度有限。
（2 分）

未充分發揮潛力
這種 MSSP 僅將機器學習流程整合在一項或其中幾項資安服務中。運用這種方法來處理資安事件相關資料考量不夠周全，只會造成服務品質參差不齊。

機器學習是供應商提供的威脅檢測與防護服務的基礎。
（3 分）

為威脅分析做好準備
這種方法可為企業提供自動化的資安策略、自動化警報處理和規劃威脅優先順序。透過裝置分析資料，可在漏洞遭到攻擊之前即時修復，並加強抵擋威脅的防護措施。這種 MSSP 可以自動處理低價值警報和噪音，可讓分析人員將更多時間用在高價值的分析上，處理影響重大的高價值警報。

計算總分

您的 MSSP 是否能夠滿足您的需求？

分數：8-15 分，能力不足的供應商

這種 MSSP 大多無法提供客戶一般期望的資安服務，可能無法依照您的需求擴展服務範圍。若要處理與法律以及產業法律合規相關問題時，其有限的服務反而讓您要處理的工作更為複雜。

分數：16-21 分，嘗試滿足各種企業需求的供應商

儘管這種供應商可能會考量您的優先需求，但其服務有所侷限，因此部分資安服務產品仍不足。您很有可能會發現遺漏的要素，並需要更全面的解決方案。

分數：22-24 分，專業知識兼具廣度與深度，訓練有素的供應商

這種供應商具備為企業量身打造解決方案的經驗，即便您並不確定自己的需求。您將獲得靈活的資安資訊和事件管理 (SIEM) 的技術選項，能夠隨著貴企業的全球擴張規模，滿足您持續變化的需求。頂尖供應商可以幫助企業在全面實施業務計畫前就瞭解到計畫中存在的風險和缺陷，他們是可靠的合作夥伴，能在世界各地為您提供豐富的專業知識和敏捷的應變能力。

選擇資安託管服務供應商時，謹記下列八項標準

企業須主動採取行動，避免自己遭到惡意攻擊。一個有效的資安計畫需要即時且嚴密的情報以及關於目前威脅情況的深層洞察。它還需要一種策略，用來管理所需資安技術的成本和複雜度，以便管理資安事件和日誌、掃描漏洞、電子郵件安全性和其他活動。然而，面對目前各式各樣的新興資安威脅，想要管理自身資訊安全的企業，往往因為缺乏必要的內部資源，而無法全天候保護線上系統。

藉由將資安業務外包給 MSSP，企業可以充分運用這些服務供應商提供的專業技術、工具和流程，大幅提升資安維護，無須大量投資在技術和資源上。但您如何選擇滿足符合您需求的 MSSP？選擇資安託管服務供應商時，謹記下列八項標準：

1. 與策略相關的漏洞分析
2. 支援多廠商且產品中立
3. 高級資安事件監控選項
4. 本機交付和全球規模
5. 行動應用程式
6. 事件應變服務
7. 雲端安全
8. 機器學習和自動化

採取後續行動

IBM® Managed Security Services 滿足所有條件，在此標準下的分數最高，能夠提供高級資安解決方案，實現接近即時的資安管理。這些解決方案包含系統和身分監控與管理、緊急應變以及全天候防護網路最嚴重的威脅。IBM 的資安服務產品組合可幫助企業降低風險、成本和複雜度，也可以幫助企業更好管理合規事宜。IBM Managed Security Services 解決方案組合包含本機安全管理與監控服務以及雲端型資安服務產品。此外，IBM 在 2019 年 Gartner 全球資安託管服務魔力象限中處於領導者地位，並在 2018 年 Forrester 的 MSSP Wave 報告中，IBM 也獲評為領導者。若要深入瞭解 IBM Managed Security Services 以及其功能，請造訪 **ibm.com/security/services/managed-security-services**