如何挑選頂尖的 EDR 產品

在端點安全市場中，許多廠商聲稱可以提供絕佳的功能。要想透過所有這些行銷和銷售手法，真正瞭解這些產品的功能，並不是一件容易的事。幸運的是，MITRE Corporation 已針對各主要端點偵測與回應 (EDR) 產品因應實際攻擊過程時表現出的偵測和調查功能進行獨立的測試。在您評估目前和未來的端點安全工具套件時，我們將區分 MITRE 的各種方法、結果，及其對貴組織的所有意義。

透過 MITRE ATT&CK 評估獲得洞察力

獨立研究機構 MITRE Corporation 發布了其 MITRE ATT&CK™ 網路安全評估的第一輪最終結果。[1] 這些評估會模擬實際攻擊者的攻擊過程，並將主要端點安全工具的偵測功能加入測試中，其中第一輪將著重於 APT-3 群組使用的技術。

在此評估中，MITRE 刻意避免直接比較廠商，而是選擇透過科學方法，針對不同的實際攻擊技術來擷取及分類各種工具的偵測和調查功能。

為了能夠深入洞悉 MITRE 的結果，Forrester Research 的資深分析師 Josh Zelonis 提供了客觀的第三方架構來評分及評估受測產品的效能。他的報告[2] 將公開評分方式套用至偵測的數量和質量以對各個廠商進行比較並分析 EDR 的市場。

在累加全部的偵測並套用 Forrester 權重後，Forrester 架構顯示 Cortex XDR™ by Palo Alto Networks 在 EDR 市場中的偵測和調查方面具有很大的優勢，提供了最佳的可視性。Cortex XDR 搭配適用於端點防護與回應的 Traps™，在許多不同領域都勝過競爭對手，包括與任何受測產品相比更大的偵測率、更小的失誤率和更為豐富的功能。

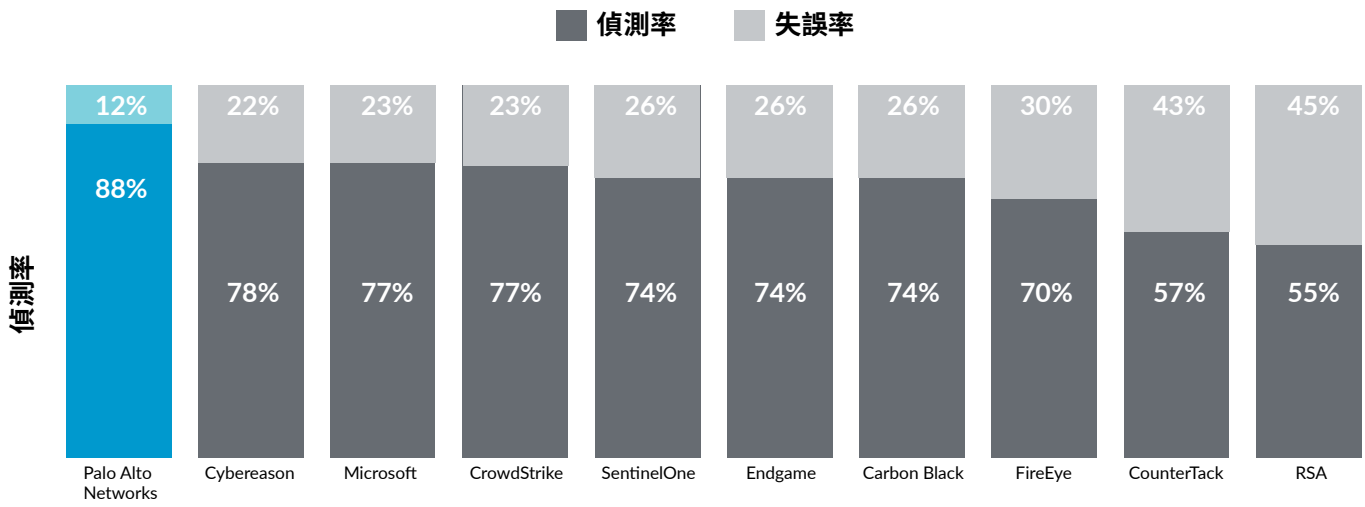

圖 1：市場中的偵測率和失誤率

新技術的評估需要量身打造並進行全面評估。在此報告中，我們將深入研究 MITRE ATT&CK 評估方法和 Forrester 的分析，以針對這些獨立公司認為重要的功能進行評估。然後，我們將針對受測的 MITRE 功能提供進一步分析，以協助您評估哪種 EDR 工具符合您的需求。

關鍵要點

- **MITRE 和 Forrester 可提供進行安全評估的起始範本。**瞭解不斷進化的威脅態勢與識別那些聲稱可提供最佳產品的廠商互相矛盾的表述同樣困難。雖然不同組織所偏重的準則並不相同，但 MITRE 和 Forrester 可提供客觀的基礎來協助各個組織瞭解其目前端點安全性和任何潛在投資的優點及缺點。
- **SecOps 團隊需要的不只是端點數據。**就算安全團隊沒有因為承擔太多的工作而筋疲力竭，仍會因為必須處理零碎的工具組合而身陷其中。將各種功能整合至強大的平台意味著更快速的回應、更佳的安全性，並可減少浪費的時間。深諳此道的 SecOps 團隊所選擇的工具應可建立各種數據來源之間的關聯性，以找出孤立工具可能忽略的威脅，包括未受管理端點中的弱點。
- **Cortex XDR 可提供絕佳的可視性。**在搭配 Traps 進行端點防護時 (已包含)，Cortex XDR 可在整個攻擊生命週期提供絕佳的偵測率，並透過失誤最少的技術提供高度關聯且零延遲的警示。此外，MITRE 只測試了 EDR 功能，但 Cortex XDR 可提供數種額外的關鍵功能，例如優異的防護以及整合網路、雲端和端點數據的能力。

1.「MITRE ATT&CK Evaluations」，MITRE Corporation，存取時間 2019 年 6 月 17 日，https://attackevals.mitre.org/evaluations.html。
2.「The Forrester MITRE ATT&CK Evaluation Guide」，Josh Zelonis 等，2019 年 5 月 21 日，https://www.forrester.com/report/The+Forrester+MITRE+ATTCK+Evaluation+Guide/-/E-RES147475。

說明第一輪的 MITRE ATT&CK 評估

MITRE ATT&CK 是一種「以實際觀察為基礎，可全球存取的攻擊手法和技術知識庫」。MITRE ATT&CK 矩陣包含了 12 種類別的數百種不同技術 (見圖 2)。在真實的攻擊情境中，攻擊者會結合這些類別中的技術邏輯序列以取得存取權限、執行命令、擷取資訊，並執行其他動作。為了模擬真實世界的情況，MITRE 會將其評估程序區分成數個輪次，每一輪都會使用已知真實攻擊者使用的一般策略和技術。

圖 2：MITRE ATT&CK 矩陣的類別

第一輪的目的在於模擬 APT-3 群組，這是一個採用精密攻擊手法的攻擊小組，經常透過瀏覽器進行入侵來獲取認證。APT-3 攻擊會密集發出鍵盤命令、控制受信任的程式，並橫向移動至其他主機。在此輪次中，MITRE 會選擇一系列的 56 Enterprise ATT&CK 技術來代表數種 APT-3 攻擊情境。

MITRE 使用可公開取得的威脅模擬工具 Cobalt Strike™ 和 Empire 來安排針對每個受測廠商進行的攻擊。MITRE 會針對每種技術記錄是否啟動偵測，並在發生偵測時記錄從最低 (無偵測) 到最高 (具有特定威脅相關資訊的警示) 規模的偵測類型。基於威脅捕捉目的而收集遙測數據但不會產生警示的工具會評分為中度規模 (見圖 3)。

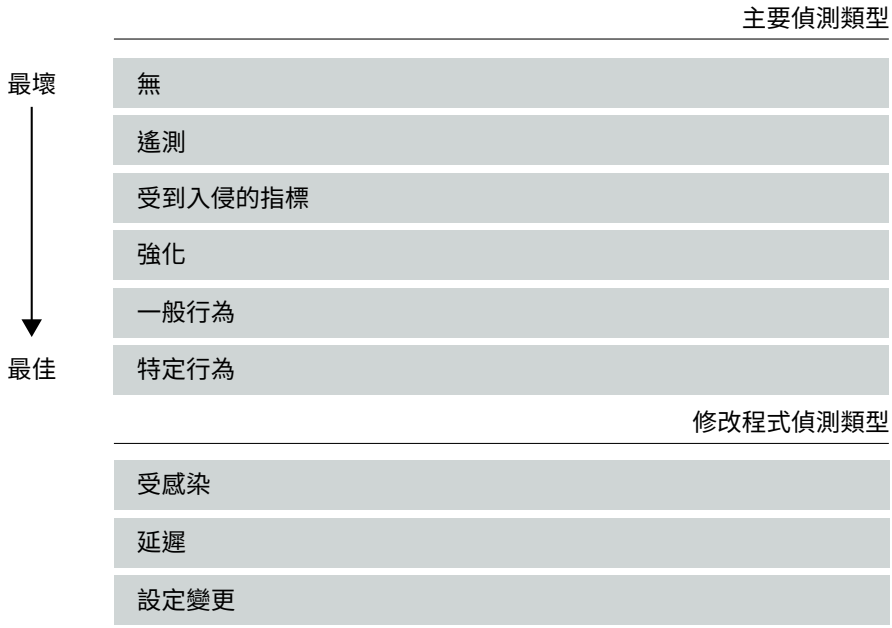

圖 3：MITRE 偵測規模

MITRE 會視需要在這些類別之上套用修改程式：

- **受感染：**基於與先前發現之惡意行為的關聯性所啟動的偵測會標示為「受感染」。這是理想狀態。
- **延遲：**偵測未即時發生，但最終仍會進行。
- **設定變更：**任何偵測僅因為廠商變更初始設定而發生。

解析 Forrester 的分析

根據上述準則，Forrester 對每個偵測進行了評分 (見圖 4)，而僅因為設定變更發生的任何偵測則為零分。

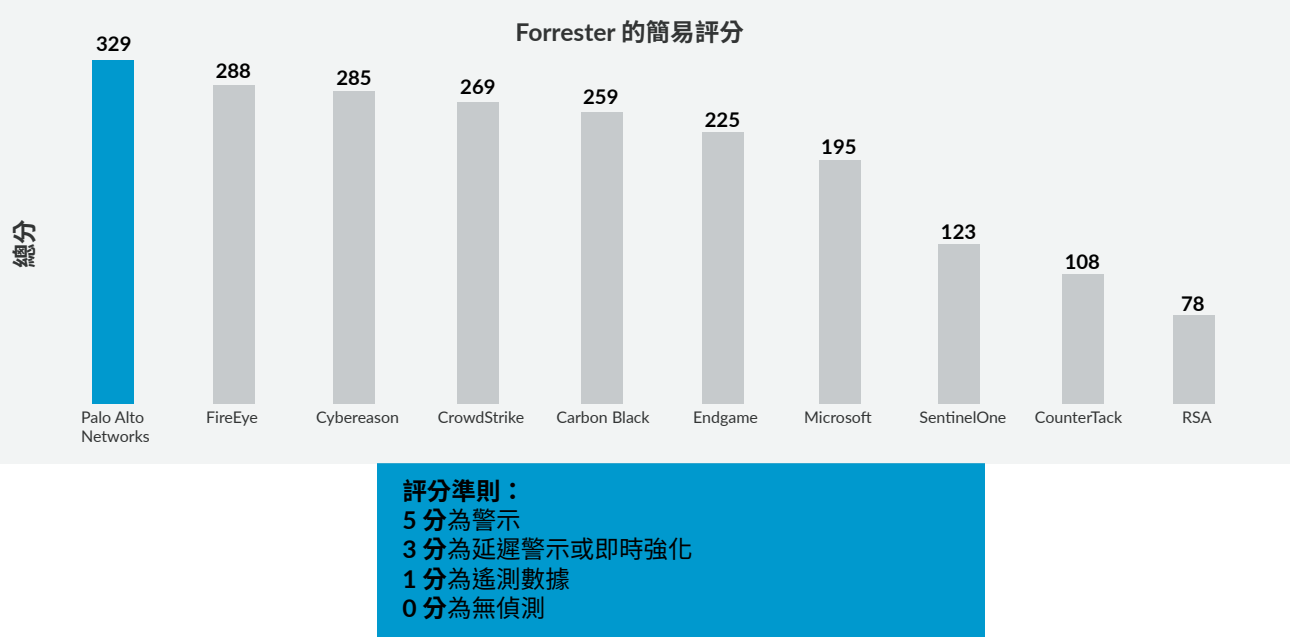

圖 4：各廠商的分數

Forrester 的評估會更為深入，並根據三個關鍵指標評估 EDR 工具和策略：

- **偵測到技術的百分比為多少？**無論偵測類型為何，其底線是能夠偵測到技術，讓分析師能夠進行調查和補救。
- **受感染偵測的百分比為多少？**在偵測的脈絡中，「受感染」一詞其實是正面的。當數據與其他惡意或可疑事件產生關連時就會被視為受感染。在本質上，幾乎不存在獨立的「惡意」動作，但以不同方式將技術整合在一起即可代表來系統中的攻擊動作。
- **產品在攻擊鏈中表現如何？**攻擊鏈 (Palo Alto Networks 將其稱為攻擊生命週期) 可描述攻擊者在一次成功的攻擊過程中必須達到的所有目標。初始存取技術的偵測及阻止非常重要，但當攻擊者遇到障礙時，他們可能會尋找其他的替代通道。在整個攻擊生命週期中評估產品可提供深層防禦的能力，並指示該工具更為成熟、涵蓋範圍更為全面。

如何執行 Cortex XDR 和 Traps

Cortex XDR 能夠發現 88.9% 的技術 (見圖 5)，136 種威脅的偵測失誤率只有 11.1%。次佳廠商的失誤率為 21%，這意味著安全團隊的盲區擴大了將近一倍。大部分的技術都會與其他的數據點產生關聯並加以強化，這意味著分析師所收到的是已脈絡化、可化為行動的警示，而非無法呈現真實威脅的獨立數據點。Cortex XDR 已展現其偵測整個攻擊生命週期的能力，且不會遺漏任何單一目標。整體而言，MITRE 評估和 Forrester 分析已充分證明 Cortex XDR 在 EDR 工具中的優越地位，並可提供無與倫比的偵測能力。

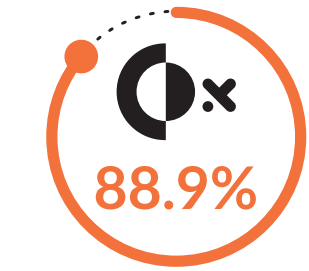

圖 5：Cortex XDR 偵測率

採用您偏好的方法

當然，目前有許多其他方法可用來分析數據。您應能深入瞭解各種工具如何滿足貴組織的特殊需求及策略。您的安全團隊可能更為偏好某些偵測類型，或對攻擊生命週期的特定部分進行優先偵測。此外，您可能會考慮一些其他的分析點。

延遲警示與即時警示

Forrester 的分析會將延遲警示和強化結合至單一類別中。不過，這些偵測並不相同，對於安全營運團隊的意義也不一樣。在許多情況下，延遲警示表示工具本身遺漏了該警示，但託管服務已監控遙測數據並在事件發生後手動產生警示。延遲警示的風險在於，必須在實際攻擊者造成損害之前加以阻止，因此無論是延遲數小時、數分鐘、甚至是數秒都至關重要。

未提供延遲警示的廠商表現出其對於技術的依賴性，而非取決於進行偵測的分析師。Cortex XDR 本身並沒有延遲警示的機制，因此彰顯出我們開發工具的策略性決策，這些工具使用強大的威脅情報、立即可用的規則和機器學習來自動進行偵測和建立關聯性。如此一來，Cortex XDR 將可有效減少平均回應時間 (見圖 6)。

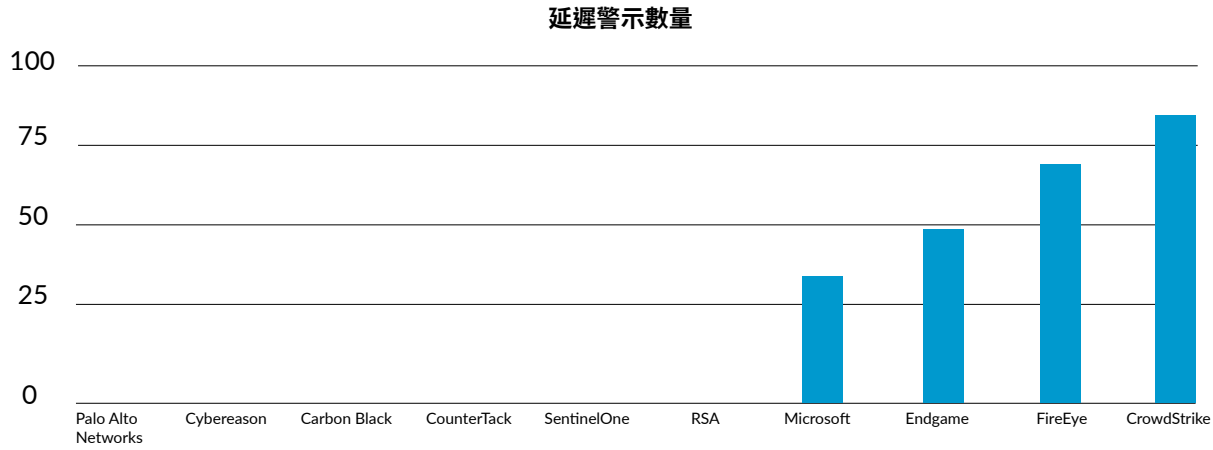

圖 6：各廠商的延遲警示數量

警示與遙測

不是所有警示都相同。根據業界評估，每次當威脅發生時，工具都會產生超過 100 則警示，這樣的誤判率會使得實際的威脅反而容易被忽視或忽略 (請注意，MITRE ATT&CK 評估並未進行誤判測試)。同時，未產生警示的 EDR 工具只適用於已能夠有效掌握目標的威脅捕捉人員。

其中應有一個平衡點。理想的工具只會產生高品質、具優先順序的特定警示。對於其他潛在 (但不一定是) 的惡意行為，EDR 工具仍會擷取遙測數據並建立關聯性以進行調查和威脅捕捉，但您可能並不想要讓工具產生很可能會造成誤判的警示。此外，您應該會希望 EDR 工具能藉由其他的脈絡來強化遙測數據，讓分析師能夠更快且更輕鬆地獲得有意義的資訊。

透過 MITRE 測試期間的預設設定，Cortex XDR 會產生 20 個即時的特定警示以及 82 個強化遙測日誌 (見圖 7)。在實際部署中，客戶可將額外的網路和雲端感測器連線至 Cortex Data Lake，使 Cortex XDR 能夠獲得對於潛在攻擊者行為的可視性和脈絡掌握，進一步降低誤判率，並提升對於惡意行為的識別能力以避免將其誤判為良性。

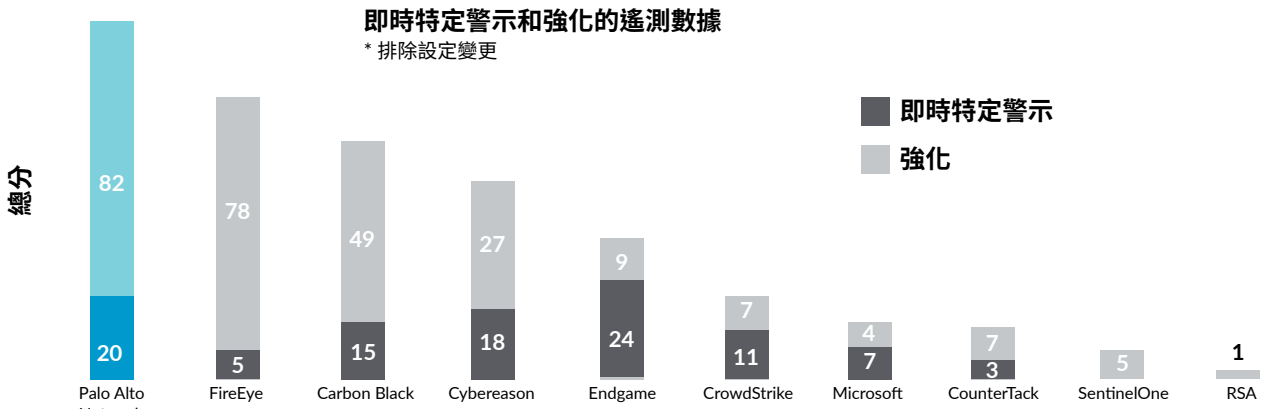

圖 7：即時特定警示和強化的遙測數據

僅有 EDR 還遠遠不夠

安全團隊經常苦於效率低下，**平均識別時間 (MTTI) 為 197 天，平均控制時間 (MTTC) 為 69 天。**[3] Ponemon Institute 發現，自從 EDR 出現之後，這種效率低下的情況反而變得更糟。增加各自孤立的工具並不是解決問題的方法。要將 EDR 建立為高效的端點安全程式，需要採用功能更加完整的整合式方法。

首先，應使用功能強大的端點防護工具進行防禦，Traps 在這方面的表現相當優異 (雖然 MITRE 測試期間已關閉防護功能)。阻止攻擊者進入您的環境永遠比事後才偵測到攻擊者來得有效。您的預防工作越確實，分析師所必須補救的意外事件也就越少。

其次就是對於基礎結構的廣泛可視性，包括 10% 至 20% 未受管理的端點，例如大部分的物聯網 (IoT) 裝置。這就是與使用者和實體行為分析 (UEBA) 以及網路流量分析 (NTA) 功能緊密整合的 EDR 的用武之地。整合的平台應能偵測到躲過第一道防線的攻擊者，並追蹤他們在整個基礎結構內的後續動作。還應該能夠識別一連串的行為是惡性行為還是良性行為。然後，它會與端點和網路防護技術分享重大發現並協調回應動作，以確保所有系統的狀態得到更新並相互合作。

簡化、整合的全方位平台才是現今安全性最佳化的正確策略，還能夠建立可擴充的安全作業來處理未來的威脅。此外，該平台能夠為您的安全分析師提供幫助，讓他們能夠專注於真正重要的工作，而避免被繁重的日常作業困擾、不得不經常排定優先順序並忽略各種合法威脅以及總在不同工具之間切換而浪費時間。

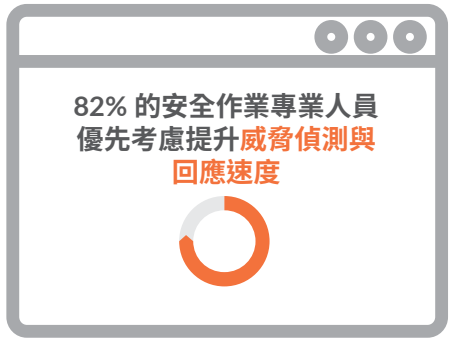

圖 8：各項 ESG 研究的 EDR 優先順序[4]

Cortex XDR 的獨特之處

Cortex XDR 是全球第一個雲端偵測與回應應用程式，可將網路、端點和雲端數據原生整合在一起，以阻止精密的攻擊。我們的 Cortex XDR 設計主要是為了協助組織來保護數位資產和使用者，同時簡化所有作業。透過無與倫比的準確性，機器學習與 AI 模型會發現包括受管理與未受管理裝置在內所有數據來源的威脅。

Cortex XDR 可提供任何警示或威脅的完整狀況以加快調查進度。它會自動將不同類型的數據整合在一起並揭露警示的根本原因，使任何經驗資歷的分析師都能夠在單一主控台中執行警示分類和事件調查。與執行點緊密整合，可讓安全團隊快速回應威脅，應用透過調查獲得的知識，進而在未來偵測類似的攻擊。

若要深入瞭解，請造訪我們的網站，或閱讀 Cortex XDR 型錄。

3.「2018 Cost of a Data Breach Study: Global Overview」，Ponemon Institute，2018 年 7 月，https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf。
4.「A Promising New Chapter in Detection and Response Tools」，Enterprise Strategy Group，2019 年 5 月 28 日，https://www.esg-global.com/blog/a-promising-new-chapter-in-detection-and-response-tools。

CORTEX BY PALO ALTO NETWORKS

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

how-to-pick-a-winner-in-edr-wp-062119