FORTINET

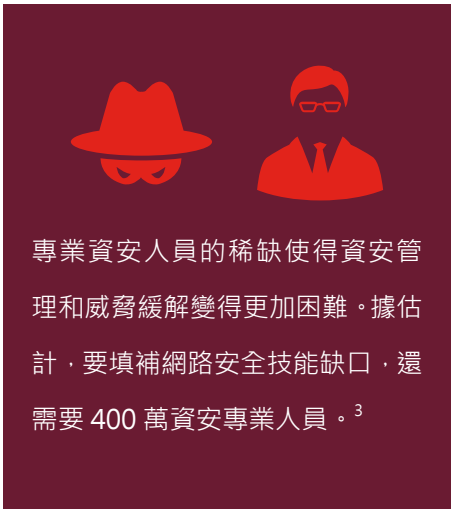
白皮書

透過整合與 XDR 解決方案掌握資安管理

不斷變化的網路威脅環境和不斷的網路安全技術，對於規模較小的 IT 安全團隊來說是一項挑戰。來自多個供應商的多種產品的複雜性，以及產生的警報數量，很容易使組織在資安上的管理不堪負荷，特別是資安技術上的短缺。

一個中等規模的組織平均使用來自不同供應商的數十個（或更多）的資安工具，這些工具每天一起產生數以千計的警報。有近一半的資安廠商 "[1] 將環境的複雜性列為最具挑戰的資安威脅原因 "，而這並不奇怪。超過四分之三的組織承認，由於未整合的資安產品，他們的資安架構是與現實脫節的。[2]

資安團隊有多個管理入口要檢查，他們必須手動連接每個入口的數據。因此，他們對警報的響應速度更慢，花時間進行的調查更少，並冒著更大的風險錯過正在進行的攻擊。



專業資安人員的稀缺使得資安管理和威脅緩解變得更加困難。據估計，要填補網路安全技能缺口，還需要 400 萬資安專業人員。[3]

降低複雜性

根據 Gartner 報告，有 80% 的公司現在和將來都計畫積極進行的資安供應商的整合。[4] 綜合的目標目的在提高營運效率或降低網路風險，同時降低成本或人員需求，但是使資安管理和降低威脅更加困難的是，專業資安人員的匱乏。根據估計，要填補網路安全的缺口，還需要 400 萬網路資安專業人員。為此，他們必須考慮平臺與個別產品的優缺點。對於大多數組織來說，整合很可能圍繞著少數的戰略平台中進行，並輔以精選的單產品，而不是極端的資安架構。

整合

依這樣的狀況，與其立即整合到一個單一的廠商，不如先第一步圍繞少量戰略安全供應商平台進行整合，(如有必要，可能選定幾個的單點產品供應商作為補充)。傳統分類上，是單點和網路做為區分，而雲端和身份管理平台則越來越多地加入進來。

當攻擊面不斷擴大和網路不斷發展的情況下，每一個資安防護都應確保能顧及到所有攻擊路徑。雖然大多數的威脅最終都是針對終端使用者的電腦、伺服器，甚至物聯網（IoT）等端點產品，但網路駭客有多種途徑可以進行入侵，大多數惡意軟體是透過電子郵件發送，其餘大部分是從網路上下載，不過網頁應用程式才是資料洩露的實際頭號來源，[5] 應用程式通常在本地或公共雲中託管，他們可能使用軟體即服務（SaaS）供應商所提供的服務，所以，如果資安防護不覆蓋整個網路的話，網路威脅將會有機會破口而入。

企業組織不僅需要擔心越來越多攻擊面的出現，還需要擔心攻擊的每個階段。當今的許多網路威脅都是多階段的，使得偵測更具挑戰性，但也提供了多種機會來檢測和防範。在多個“網路殺傷鏈”階段部署技術可以建立深度防禦，從而加強資安廠商整合所帶來的收益。

更快偵測與回應威脅

然而，正如一位知名分析師所指出，資安是一個相對 " 年輕 " 的行業，它仍在走向成熟中。事實上，直到現在，網路、電子郵件、端點、雲端等多個安全平台才在跨層次偵測與回應平台（XDR）概念架構下走到一起。

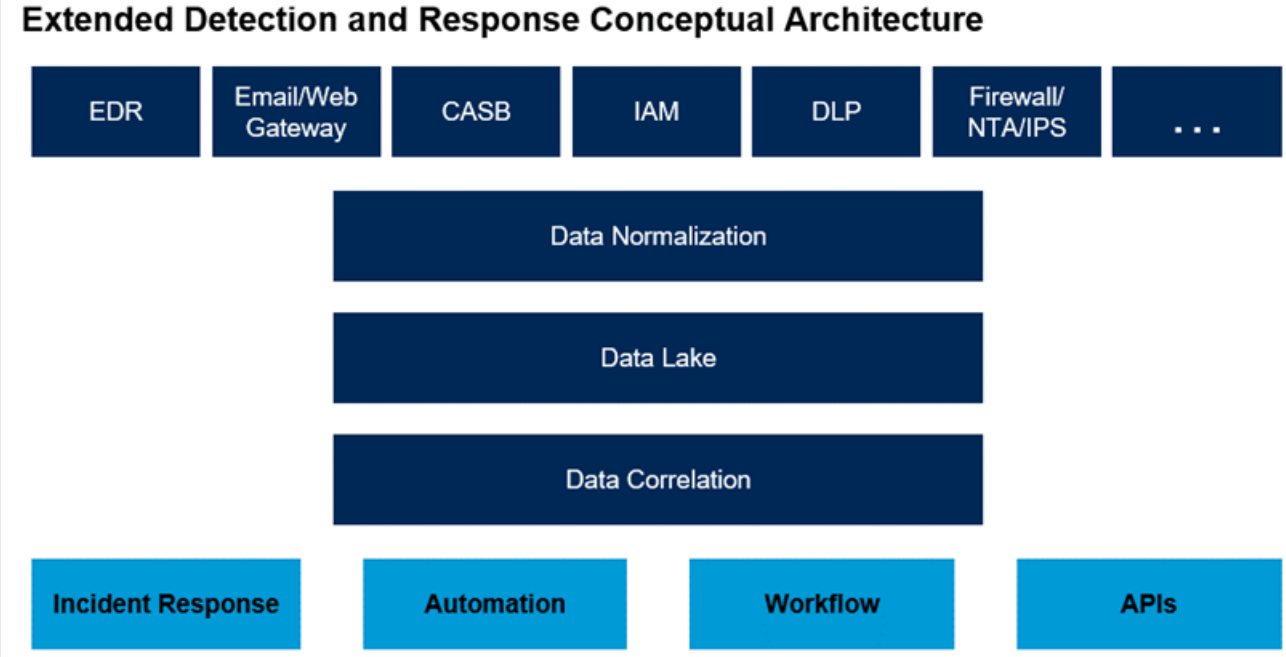


圖 1：Gartner innovation insight for XDR，2020 年 3 月。

一個有效的 XDR 解決方案能夠跨安全控制收集、正規化和關聯資料。它可以幫助資安團隊更快地發現威脅、協助調查，並加快響應速度。然而，XDR 仍是一個新概念，各種方法皆不相同。比如在輸入數據湖的安全控制面的廣度、採用協助調查還是自動調查、自動化程度與協調反應的程度、以及整個系統的有效性與哪些安全控制需要合併等等。

總結

依目前來說，針對 XDR 早期的研究仍持續進行中。透過綜合和有效的 XDR 解決方案，企業可以極大地改善安全態勢並提高營運效率。有關 XDR 解決方案的詳細資訊，歡迎關注並追踪 Fortinet “選擇 XDR 解決方案時的五大注意事項”，您將會有更多收獲！

[1] “Center Security On Advanced Technology: How A Technology-Led Strategy Helps CISOs Successfully Secure Their Organizations,” Forrester, July 2017.

[2] “The CIO and Cybersecurity: A Report on Current Priorities and Challenges,” Fortinet, May 23, 2019.

[3] “(ISC)² Estimates Cybersecurity Workforce at 2.8 Million,” (ISC)², November 6, 2019.

[4] John Watts and Peter Firstbrook, “Security Vendor Consolidation Trends: Should You Pursue a Consolidation Strategy?” Gartner, July 30, 2020.

[5] “2020 Data Breach Investigations Report,” Verizon, May 2020.

859744-0-0-TW
D:\00- (20210102)____Fortinet-20210127____DM (Paid Search)\wp-FA-take-control-of-security-operations-with-consolidation-and-xdr-12152020\wp-FA-take-control-of-security-operations-with-consolidation-and-xdr-12152020