解決方案簡介

利用 FortiXDR 實現威脅檢測、偵查和回應的完全自動化

簡介

長久以來，企業應對新興網路威脅的方式就是不斷添購新的資安產品。雖然許多情況下這些產品有效，但作為一個網路整體架構，面對不同廠商的資安產品所帶來不同的管理方式，也使得在監控和資安策略與採取的行動上都有所不同，這已經讓資安團隊變得不堪重負。

令人更為擔憂的是，潛在的網路攻擊風險也將因此不斷增加，這些攻擊到處躲閃，從各設備的縫細中溜走，或在監測中被遺漏或消失。縱使到了現今，大多數的企業仍在苦腦著供應商整合，主要希望能在兼顧安全外，還能提高營運效率，然而有效的整體解決方案才是成功的解決之道，而非來自湊合的各家產品，這就是 FortiXDR 可以提供幫助的地方。FortiXDR 為新世代跨層次偵測與回應平台，建立在廣泛、整合、自動化的 Fortinet 安全織網之上，具有完全自動化的威脅檢測、偵查和回應功能，有助於企業提高安全態勢與營運效率，減輕資安團隊的負擔。

新世代跨層次檢測與回應平台

根據 Gartner 的統計，80% 的企業目前或計劃在未來兩到三年內整合旗下的安全供應商。

越來越多的企業偏向採用 XDR 這樣的解決方案整合不同廠商的資安設備，FortiXDR 可將您的 Fortinet 安全織網快速轉換為 XDR 解決方案，橫跨組織單位的安全部署，直接將訊息集中到管理中心，各項分析自動檢測潛在的高風險事件，並同時啟動分類偵查，另外可預先定義回應管理，處理適當的補救和響應。以上過程全部自動化，減少大量無用的警報，大大減輕資安人員的負擔。

部署廣泛的安全織網

Fortinet 的安全織網部署可覆蓋整個數位化組織，包括：

- 各個端點和用戶的端點保護（EPP）與身份存取管理（IAM）。
- 有線交換機、無線接入點及企業防火牆網路和接入層
- 雲端存取安全代理（CASB）、Web 應用防火牆（WAF）與安全電子郵件閘道（SEG）

Fortinet 所有產品都已完成整合，並且可將相關數據統一傳送到控制台上。

全面檢測分析

FortiGuard 實驗室的專家們開發了一套豐富且不斷增加的高級分析方法，目的在識別網路攻擊的早期潛在指標，並應用到集中化、規範化、相關的遙測數據。這些檢測開始了事件偵查的下一個階段。

由人工智慧（AI）驅動的檢測功能

根據初始檢測的類型，自動偵查過程將由 AI 驅動的決策引擎動態跟蹤，從而複製仿真人的安全分析師進行採取專家行動。決策引擎能夠調用廣泛的微服務，提供豐富和進一步的分析。一些常見的例子包括來自 FortiGuard 實驗室和協力廠商的威脅情報、文件分析 (如靜態 Yara 規則或動態沙箱評估、社群聲譽或用戶行為基線)。

預先定義的反應框架

企業可以選擇預先設置策略，這些策略將根據分類、用戶群組、風險暴露和其他標準來定義想要採取的行動，這可加快了回應的速度與補救措施。

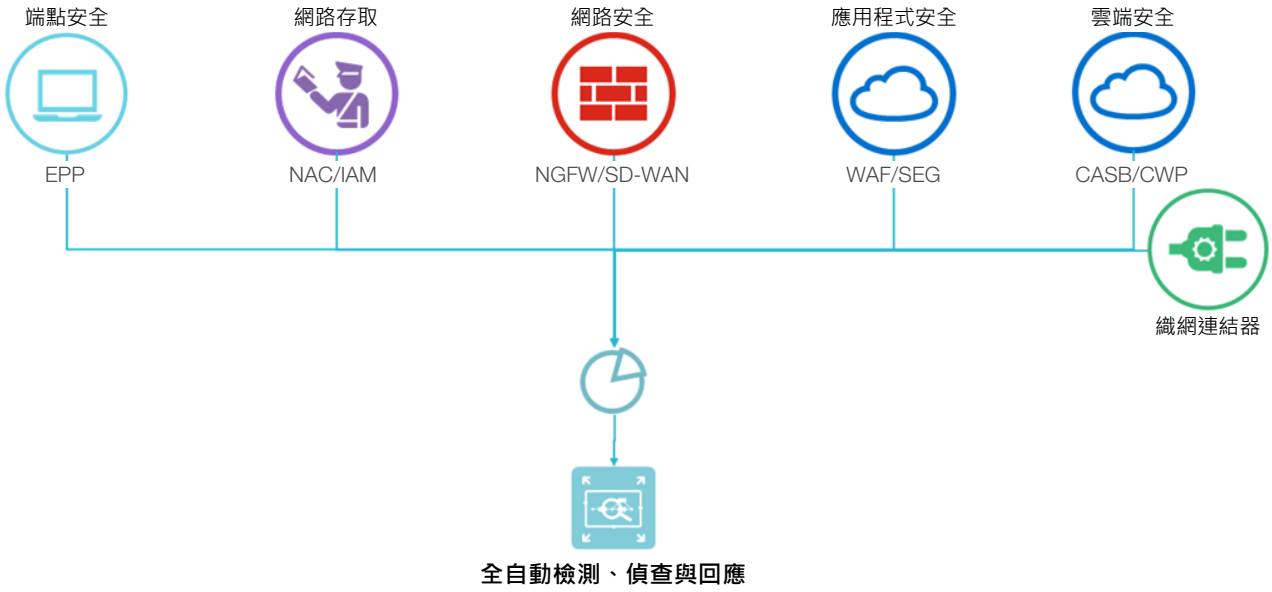

圖 1：FortiXDR 與 Fortinet 安全織網 Fabric.

FortiXDR 的不同之處

XDR 是一個早期的概念，也是業界的熱門話題。然而，它與我們的安全織網願景完全一致，使我們的解決方案具有許多先天優勢，這些優勢包括覆蓋面的廣度、各個組件的有效性和自動化的程度。因此，企業更有可能實現不同廠商產品整合的好處。

覆蓋範圍的廣度

越是可以進一步“擴充”的 XDR 解決方案，越是可以獲得更多的訊息用於分析、充實和進行分類。雖然網路和端點元件是 XDR 的防護基礎，但是涵蓋資訊存取、電子郵件、網路應用和雲端的能力的 FortiXDR 更加與眾不同，在早期和後續擴大檢測範圍以覆蓋整個網路的能力是一個顯著優勢。值得注意的是，FortiXDR 擁有偵察檢測詐欺的洞察力，並且根據我們的代理用戶和實體行為分析（UEBA）的後期數據監測加以補充，讓防護獲得更多保障。

平均而言，FortiXDR 將 100 個高價值的個別警報轉換為 10 個高保真的事件檢測，以便進一步偵查和回應。

有效發揮不同元件設備

企業無需擔心在部署 Fortinet 安全控制中心和 XDR 後會導致不同廠商元件產生衝突。所有接入 FortiXDR 的 Fortinet 資安產品在獨立測試中一直都獲得最高分。他們在 AV-Comparatives、ICSA 實驗室、NSS 實驗室、Virus Bulletin 等第三方的測試中表現出業界領先的整合性能。事實上，Fortinet 的產品組合是業界中最突出的認證產品。

自動化程度

當然，重要的是要發現威脅的存在，否則威脅被忽視將為企業造成巨大損害。然而，大多數資安團隊最不需要的就是一堆無效的警報。一些廠商採取的作法是在關聯地方跳出更多安全警告，當然也有一些漂亮的視覺化圖表，而 Fortinet 已經遠遠超出了這個範疇。FortiXDR 不僅實現了相關性資料規範化和完全檢測分析自動化，同時還實現了事件偵查、分類和修復過程的自動化。因此，FortiXDR 為資安團隊不僅減輕工作壓力，更加提高網路安全狀況。

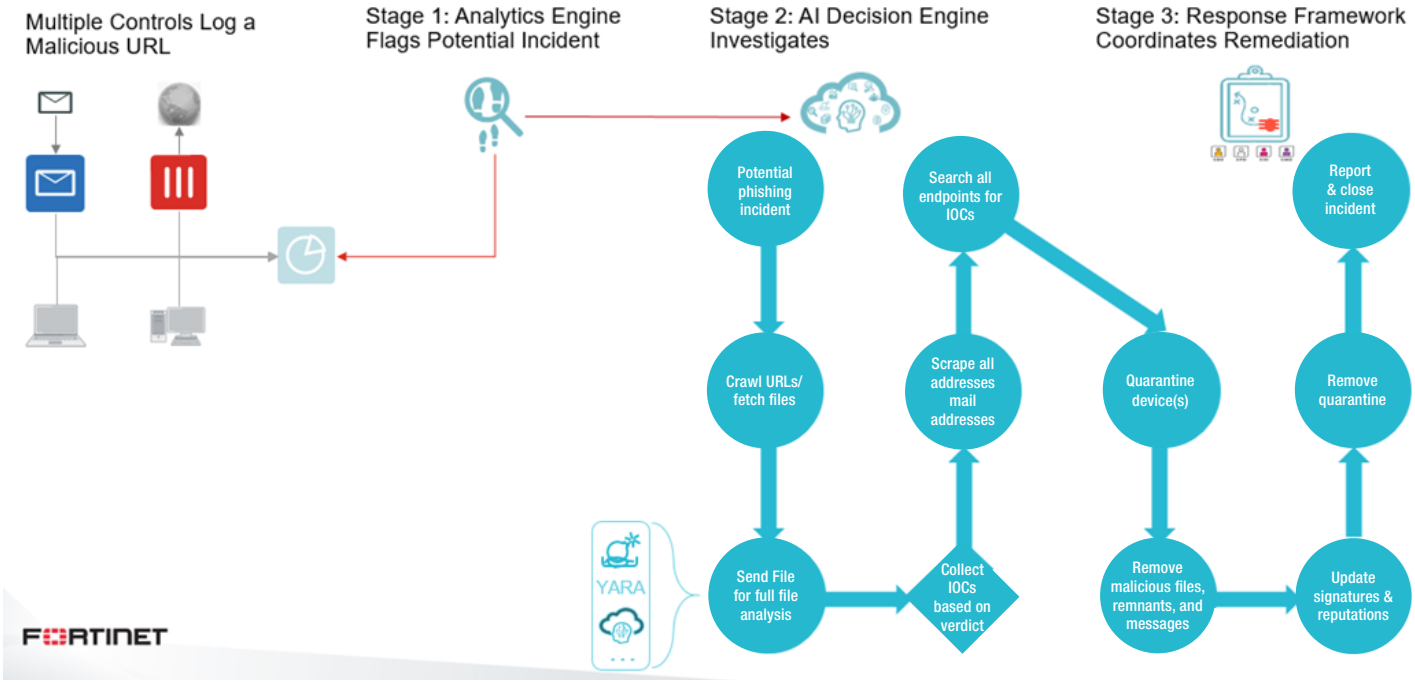

圖 2：網路釣魚檢測、偵查和回應。

利用 FortiXDR 提高安全態勢和營運效率

在資安人員短缺的情況下，當今網路威脅的數量、複雜性和產生速度都不斷的增加，資安團隊面臨的挑戰比以往任何時候都來的大。由於有這麼多各自獨立的資安產品需一起管理，因此需要一種整合企業旗下資安產品的方法，這就是為什麼如此多的企業正在追求設備的整合，以及為什麼像 XDR 這樣的新解決方案會出現在市場上。FortiXDR 採取了一個獨特的方法，除了能將不同資安產品進行整合外，更將檢測、偵查和回應過程完全自動化，可在洩露數據或勒索成功之前即識別出網路攻擊，除了減輕資安團隊的負擔，也使人員們能夠有更多時間思考與規劃更有價值的資安策略，來保護企業安全。

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

FORTINET

www.fortinet.com/tw

May 7, 2021 10:42 AM

859551-0-0-TW