產品型錄

Symantec Endpoint Threat Defense for Active Directory

Active Directory：網域入侵根源

Microsoft Active Directory 是全球 90% 企業使用的網路網域服務，用於管理及控制企業內部資源，例如伺服器、端點、應用程式及使用者[1]。Active Directory (AD) 的設計是開放給任何網域連線使用者，亦即公司網路上的所有身分及資源都會遭到暴露，讓 AD 成為攻擊者的首要目標。

只要有一個受入侵的端點連線至企業網域，就會危及整個組織：

- 想知道敏感資料在哪裡嗎？
- 想知道管理員在哪裡嗎？
- 想知道如何掌控目標環境嗎？

只要透過 Microsoft Active Directory 即可。

一旦能夠進入連線網域的端點，攻擊者就能對 AD 資料庫執行偵查，掌握所有組織資源。下一步就是竊取儲存於端點本機或遠端其他資源的網域憑證。攻擊者竊取憑證時，能夠完整及秘密存取企業組織內部的所有伺服器、應用程式及電腦，最終目標是竊取或加密資料。

攻擊者在刺探利用之後，會使用受信任的應用程式和內建工具；由於使用受信任應用程式及內建通訊協定，而不是使用惡意二進位檔，因此幾乎不可能進行這類秘密攻擊的偵測、鑑識追蹤及搜尋等行動。

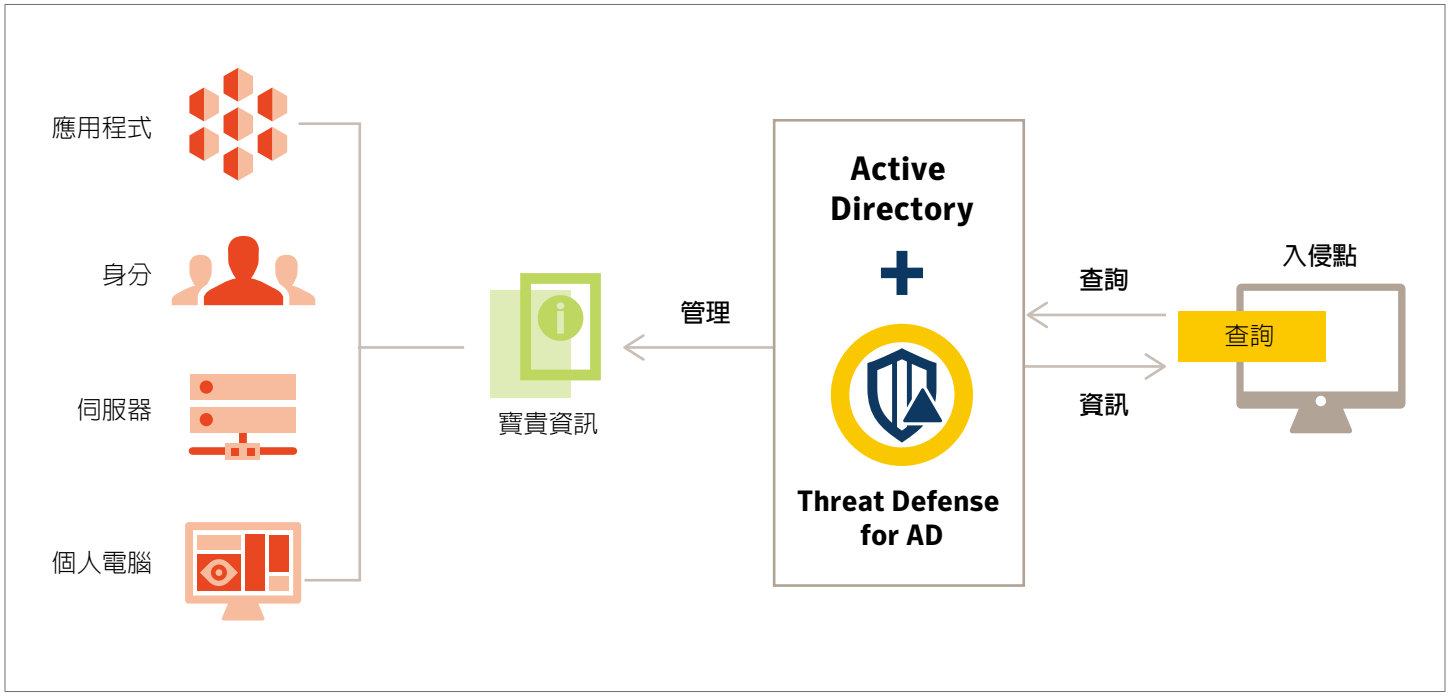
強化 Active Directory 以限制 APT

Symantec Endpoint Threat Defense for Active Directory (Endpoint Threat Defense for AD) 讓賽門鐵克的端點安全解決方案更上層樓，由端點提供有效的 Active Directory 防禦，因應各種秘密攻擊或 APT，以提供自動入侵遏止、資安事端回應及網域安全評估等功能。

這是唯一的安全解決方案，能在攻擊者入侵端點後加以遏止，不會讓攻擊者存留在網域中。本解決方案可中斷偵查活動，避免攻擊者利用 Active Directory 橫向移動至其他資產。Threat Defense for AD 可因應現今網路的最短抵抗路徑，大幅減少在端點這入侵起源偵測及遏止的時間、工作與錯誤。

Threat Defense for AD 應用 AI 導向的原生語言處理、精密的混淆技術，以及先進的鑑識方法，迅速探索及遏止入侵。

[1] Active Directory 概觀 (An Overview of Active Directory)，Philippe Beraud，Microsoft Corporation，2016 年



利用混淆技術對抗攻擊，防禦 Active Directory

Threat Defense for AD 可有效在入侵點控制攻擊者掌握企業組織內部資源，包括所有端點、伺服器、使用者、應用程式及本機儲存憑證。賽門鐵克解決方案可自動學習企業組織完整的 Active Directory 結構 (伺服器、端點、應用程式、使用者、分公司、命名慣例、設定、屬性等等)，並利用此資料建立可靠且不受限制的混淆效果。在端點會進行程序、內容及 Active Directory 活動的執行階段評估，以判定是否需要啟用混淆功能。混淆功能可讓遭入侵網域連線資產的觀點投射至攻擊者；攻擊者在 Threat Defense for AD 的掌握下與資產互動，或嘗試使用網域管理員憑證，洩漏本身行蹤。此時將觸發高準確度警示，並自動封鎖攻擊。

即時入侵能見度及自動化攻擊遏止

攻擊遭到偵測時，就會由端點觸發警示，並由隨選掃描收集攻擊相關的特定鑑識資訊。只在攻擊遭到偵測時，才自動進行鑑識程序及掃描適當資訊，可保證只出現高度優先的正當警示，減少警示疲乏。

本解決方案使用獨特的資安事端回應方法，專為企業 AD 網域環境所設計，可提供即時鑑識報告，掌握攻擊者的實際偵查、憑證竊取，以及橫向移動階段。其中將完整記錄攻擊鏈，一路追溯至原發資安事端，識別攻擊起源，並評估攻擊是否為當地資安事端，或是更大規模事件的一部分。自動緩和功能可停止端點的惡意程序，即時遏止入侵，使其無法繁衍影響其他程序、覆寫其他部分的記憶體、執行偵查指令，或是與網路通訊。

持續評估 Active Directory 以減少攻擊面

隨著企業組織實作的 Active Directory 演進發展，組態設定可能沒有適當維持、安全性強化可能並未實作，而網域及 Active Directory 服務可能開始出現漏洞，成為攻擊者利用的目標。此外，攻擊者可能會留下後門及持續存在的陷阱，以便隨時再次返回。Threat Defense for AD 會持續探測網域的不當設定、漏洞及持續性，並由攻擊者觀點向 Active Directory 管理員呈現其網域狀態，以便立即緩和風險減少攻擊面。

自動化評估程序利用攻擊模擬，收集網域設定、權限帳戶、安全性設定、GPO、端點、網域控制器及 Kerberos 的深入資訊，然後自動分析網域及 Active Directory 架構的每個元件，確認是否有設定不當的地方，以及攻擊者是否在其中留下後門。持續識別這些不當設定及後門相當重要，以降低網域風險。一旦找出不當設定或後門，就會傳送警示至中央主控台，提出各種規定建議或矯正方式。

若要進一步瞭解 Symantec Endpoint Threat Defense for Active Directory，請造訪 http://www.go.symantec.com/threat-defense-for-ad

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的策略性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。

若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或

賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號
電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw

19C199995_DS_SEP_THREAT_DEFENSE_AD_TW