# 賽門鐵克的 EDR 與 XDR 介紹

## EDR 的誕生

EDR 是 Endpoint Detection and Response 的簡稱，也就是端點偵測與回應。EDR 是大家耳熟能詳的提升現有企業防毒或企業端點防護/安全……等必要防護措施、最被人推薦的更高階等級的安全防護以及端點資安持續監控與異常反應系統。EDR 的誕生驅使於企業組織希望能有一種解決方案能在萬一如果發生資安事故時，可以在最短的時間內找到問題之根源，不會毫無頭緒地像無頭蒼蠅般處理善後。其次是遵循法規要求，幾乎所有先進國家皆規定對國家基礎架構、金融、高科技產業以及特定的產業規定要建置 EDR 系統，以立法來規範與強制企業強化資安治理，來善盡社會責任與強化國力。另外，提高安全性也常常是評比EDR的重要項目。

特別是美國國家標準技術局 (NIST) 於 2014 所發布網路安全框架 (Cybersecurity Framework) 的 5 大核心--識別 (Identify)：明確知道重要資訊資產放在哪裡、保護 (Protect)：攔截對內的攻擊、偵測 (Detect)：發現入侵、回應 (Respond)：遏止及矯正問題與復原 (Recover)：恢復正常運作。定義了企業建構網路安全防護時，所需要重視的 5 大構面，讓企業在管理安全風險時，能夠對應到事前、事中與事後的環節，提供網路安全生命週期的管理策略。NIST 的網路安全框架更是 EDR 被列為企業資安必要解決方案的最大推手。

## EDR 能再提升防護安全性等級

首先，我們先來驗證為何 EDR 能提升現有端點防護安全性的真實性。企業目前大都已採用像是賽門鐵克端點防護 (SEP：Symantec Endpoint Protection) 之類的企業防毒／端點防護/端點安全解決方案。如果還想在端點上再提升安全等級，唯一也是最佳的解決方案就是 EDR。賽門鐵克的 EDR 具有業界獨特的雲端雙沙箱：實體沙箱以及虛擬沙箱，沙箱的功能是當無法百分之百辨識一個全新的檔案是安全或風險時，我們就開啟／執行它，到底會發生什麼事情，是否會衍生後續一連串的感染鏈(沙箱就如同現實生活中軍警發現疑似爆裂物之撤離現場人員，設置警戒範圍，禁止任何人接近以及後續的引爆。爆裂物引爆方法很多，目前多以水銀、定時、電池、引擎、遙控等方式引爆電雷管，造成爆炸)。業界大家都只採用虛擬沙箱，國家支援以及企業化經營的 APT 頑強駭客組織，也知道大家的沙箱都是採用虛擬沙箱，所以在釋放出惡意程式之前，就先測試所有廠牌的防毒軟體偵測不到以及自己會辨識是否進入虛擬的環境，如果發現虛擬環境就直接裝死，業界稱這種防偵測技術為虛擬認知 (Virtual Awareness)，所以即便有導入沙箱，還是有一定比例的漏網之魚。賽門鐵克的雲端沙箱運行在遍及全球的 Google Cloud 雲端基礎架構上的優勢，這與自建在地端的沙箱以及行銷宣傳式的辨識特定駭客工具組合的模擬器被誇大誤導為類沙箱的端點防護技術有很大的天壤之別。事實證明，賽門鐵克獨特的實體沙箱能有效偵測具有虛擬認知的反偵測技術，比業界約高出 15%-45% 左右的偵測率。這一段可以說明 EDR 在提升防護能力有憑有據的運作原理與邏輯。

接著，我們來了解 EDR 為何可以針對目標式的 APT 攻擊提早預警，以及萬一發生資安事故，EDR 是如何發揮人工智慧、機器學習以及先進演算法來解析資安事故的脈絡，重構感染鏈以幫助資安人員可以快速找到根因。我們都知道，在還沒有導入 EDR 之前，萬一發生資安事故，多數的企業是無法自力找出根因的，即便巨資緊急外聘資安事故鑑識廠商，也要花上好幾天甚至上月才有辦法獲得證據不足的結論。EDR 的底層邏輯就是關聯分析與交叉比對。賽門鐵克的 EDR 會將所有端點的系統日誌以及端點防護的安全日誌全部記錄下來，透過關聯分析與交叉比對，就跟路口、公車亭採用的網路攝影機一樣，許多複雜棘手的社會案件多是透過這個系統的完整記錄及關聯分析與交叉比對才能快速破案。當然關聯分析、交叉比對雖然只有短短的八個字，但每一家廠商的技術與競爭優勢各有不同。以賽門鐵克為例，由於我們分析的資料點橫跨端點安全軟體的安全日誌、系統日誌以及參照我們全球最大的民營資安威脅情報網路資料庫 (GIN：Global Intelligence Network)。GIN 彙整包含端點、電子郵件、網頁等數億個使用者的威脅情報、全球駭客集團過往以及最新的攻擊策略、技術及程序 (Tactics, Techniques, and Procedures，TTPs) 讓賽門鐵克的 EDR 可以更快速偵測、應對，使防禦從被動變為主動。由於參照的資料點是業界最多的，就如同資料庫的欄位越多，可以篩選的結果，就越能精準滿足你的需求。同樣的道理，因為參照的資料點是業界最廣的，賽門鐵克的 EDR 給的建議與指導準則也是最精準的，不會有模稜兩可或語意不清可以免除資安人員的決策疲勞與時間壓力。偶發性的隨機攻擊與目標式的 APT 攻擊之結局是天壤之別。在指標性的企業或政

府部門發生重大資安事故時，如果沒有導入 EDR 以充足明確的證據來證明事故的脈絡、攻擊者的動機與能力以及嚴重與否，恐將會淪為含糊其辭、自圓其說的窘境。

最後，就跟醫療與藥品一樣，先講求不傷身再來才是療效。導入任何一個全新的解決方案，最擔心的就是需不需要變動現有的基礎架構，會不會改變現有的操作習慣，有多高的機率會發生未知的問題。對現有賽門鐵克端點防護 (SEP) 的用戶提升至 EDR，完全不用擔心前述的種種風險。因為 EDR 與 SEP 共用代理程式，所以不需要再安裝任何代理程式，當然也就沒有任何與現有軟體或系統有相衝突或不相容的風險。EDRM(EDR 主控台) 與 SEPM(SEP 管理主控台) 協同運作，所以地端自建的環境，只要再安裝一台 EDRM 就可以了。如果是雲端版本，完全不用安裝 EDRM，只要憑帳號登入原廠的雲端主控台即可。所以導入 EDR 是可以非常容易上線的，完全不用考慮影響層面。

## 功能性整合的跨界延伸 XDR

在評估 EDR 的當下，也常常會聽到 XDR 這個名詞。有些廠商的端點 EDR 解決方案名稱就稱為 XDR，並非功能性整合的跨界延伸 XDR：Extended Detection and Response。而賽門鐵克所定義的 XDR 就是功能性整合的跨界延伸 (Cross-X) 端點 (EDR)、電子郵件 (Email DR)、網頁 (Web DR) 以及網路 (Network DR) 的偵測 (Detection) 與回應 (Response)，功能性整合的跨界延伸的 XDR 可比喻為從海、陸、空以及認知作戰的情資彙整出更完整具體的攻擊樣貌。如果同時採用賽門鐵克的郵件安全雲端服務以及網頁安全與分類雲端服務，就能整合 Symantec CASB／CloudSOC 從單一雲端主控台更完整地全攬全局，可有效地拆解來自端點、郵件、網頁或網路的攻擊鏈。所以賽門鐵克是業界涵蓋範圍最廣的 XDR 深厚功力之領導業者，而非把 EDR 命名為 XRD 的行銷導向的廠商。當然，也偶有賽門鐵克的用戶在導入第三方 EDR之後才發現並後悔，原來第三方 EDR 廠商對比的賽門鐵克解決方案是 SEP，而非 EDR。就好像現有的國民車拿來與豪華車比較一樣，但像這種妥善率最高、養車成本最低的賽門鐵克品牌推出的國民車 (SEP)，其所推出的豪華車 (EDR) 也一定是「專注完美，近乎苛求」。

## 結論--賽門鐵克 EDR 優勢說明

**架構簡單：**

- 部署設備簡單，並且可以在實體與虛擬環境安裝，如採用原廠雲端架構，則無需自行安裝主控台。
- 無需額外安裝 Agent。

**更佳偵測：**

- 透過雲端沙箱可以快速偵測，並透過實體與虛擬沙箱找出真正的惡意程式。
- 自動化 Cynic 分析。

**更快處置：**

- 可以透過端點、郵件、閘道快速找出高風險事件。
- 透過 IoC 快速搜尋 (檔案名稱、機碼、HASH……)。

**單一管控平台：**

- 透過單一管控平台可以同時監控端點、郵件、閘道。

**～導入賽門鐵克解決方案，當然找業界公認的賽門鐵克解決方案專家--保安資訊有限公司～**

## 關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片 ) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。( 美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員 )。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

## 關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。