產品型錄

Endpoint Detection and Response Cloud
雲端端點偵測與回應

完整端點能見度和自動化威脅搜尋

快速一覽

偵測 – 搜尋不屬於此環境的不速之客

- 偵測基本活動之外的軟體、記憶體、使用者和網路不速之客
- 使用時間表和路徑分析來偵測多階段式攻擊
- 運用程序記憶體分析來揭露針對記憶體的攻擊

自動化 – 利用技術純熟的調查人員所採用的最佳實務準則

- 運用自動化資安事端教戰守則中的規則，來複製技術純熟的調查人員採用的最佳實務準則和分析
- 運用自動化跡象收集，取得端點活動的深入能見度
- 運用內建的教戰守則，發起網路安全功能，學習專業調查方法

視覺化 – 將大量網路資料轉化為可採取行動的結果

- 透過視覺化連結分析，瞭解不相關的資料類型之間有何情境關係
- 使用圖形式警示，快速學習資安事端的來源、時間和影響
- 將大量端點遙測資料轉化為互動式圖形，以便側重於相關活動

簡介

安全團隊會遭遇「隱匿行蹤」的複雜攻擊，這些複雜攻擊往往藏在客戶環境中，潛伏時間可能長達 190 天[1]。攻擊者更頻繁地運用隱匿性技術在客戶環境中任意行動，例如：使用竊取而來的憑證偽裝成合法使用者。零時差搜尋的案例出現微幅下滑，而「自給自足」戰術卻日益增加，這類戰術不需仰賴惡意軟體攻擊漏洞的傳統組合。這些戰術由於使用合法工具，因此更加難以偵測[1]。

企業需要新的方法來偵測這些可能成為漏網之魚的威脅。此外，若要尋找技術純熟的人員來執行深入調查，將極為困難且耗費龐大成本；即便您的企業旗下擁有這些內部技術人才，留住這些員工也相當困難。

Endpoint Detection and Response Cloud (EDR Cloud) 概述

賽門鐵克雲端端點偵測與回應 (EDR Cloud)，能在整個企業環境提供深度端點能見度、自動化威脅搜尋和入侵回應。賽門鐵克 EDR Cloud 是能在數分鐘內部署完成的雲端式服務，可協助加強企業的安全態勢，抵禦網路攻擊。賽門鐵克 EDR 雲端，運用豐富的規則和使用者行為分析，提高調查人員的生產力，並將最有經驗的安全分析師所握有的技能和最佳實務準則帶給任何企業組織，進而大幅降低成本。

安全團隊運用支援隱匿威脅偵測的鑑識分析和內建的教戰守則，能快速發起調查，並運用經過充分設定的時間點掃描，無須額外部署代理程式。

搜尋不屬於此環境的不速之客

賽門鐵克 EDR 提供軟體、記憶體、使用者和網路基本活動的全面性檢視，進而簡化環境內的攻擊者搜尋。當攻擊者在環境中有所行動，他們的惡意軟體和使用者活動便顯示為異常。賽門鐵克 EDR 雲端會偵測這些環境中的不速之客，包括：

- 軟體異常 – 揭露安裝罕見軟體、組建不一致、搭載老舊或未修補作業系統 (OS) 版本的端點
- 記憶體異常 – 運用程序記憶體、檔案和 OS 物件及系統設定的鑑識調查，偵測記憶體內的不速之客
- 使用者異常 – 使用者行為分析，能偵測偽裝成合法使用者卻執行異常活動的攻擊者
- 網路異常 – 運用數據分析來辨識異常 IP 位址，另一方面運用信譽查詢來辨識與資料洩漏相關的 IP 位址和網域

此外，賽門鐵克 EDR Cloud 包含數個威脅引擎，能為檔案、使用者帳戶和網路連線產生風險分數。偵測功能亦包括：

- 使用數百萬個正常與惡意檔案的神經網路式機器學習
- 由客戶提供的第三方威脅情報來源
- 針對登錄變更和排定的工作進行檢查，協助揭露持續式威脅
- 多個防惡意軟體引擎

運用技術純熟的調查人員所採用的最佳實務準則

賽門鐵克 EDR Cloud 支援教戰守則，能夠自動化安全分析師的複雜多步驟調查工作流程。內建教戰守則，可快速揭露可疑行為、未知威脅、橫向移動和政策違規。安全團隊可以檢視教戰守則來學習專家級搜尋和調查技術。此外，調查人員可以建立自己的教戰守則，以便自動化最佳實務準則和針對特定文件的威脅搜尋情境。

將大量網路資料轉化為可採取行動的結果

賽門鐵克 EDR Cloud 擁有強大的視覺化功能。系統提供了視覺化連結分析，並搭配互動式圖形，就此改變安全專業人士使用和參照電腦和網路資料的方式。

機器輔助分析，提供了與所有相關資料進行大規模互動的能力。連結分析功能，可以針對不同資料類型間的複雜關係提供快速的概念化聯想。

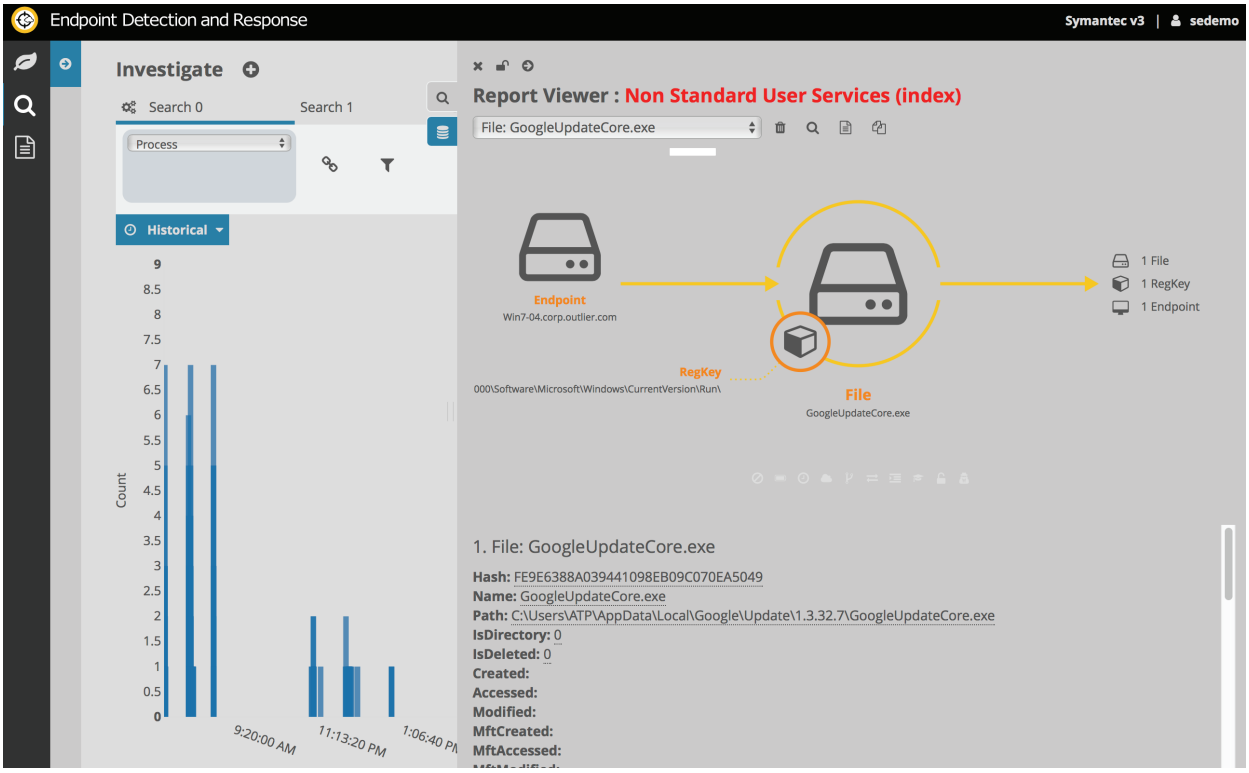
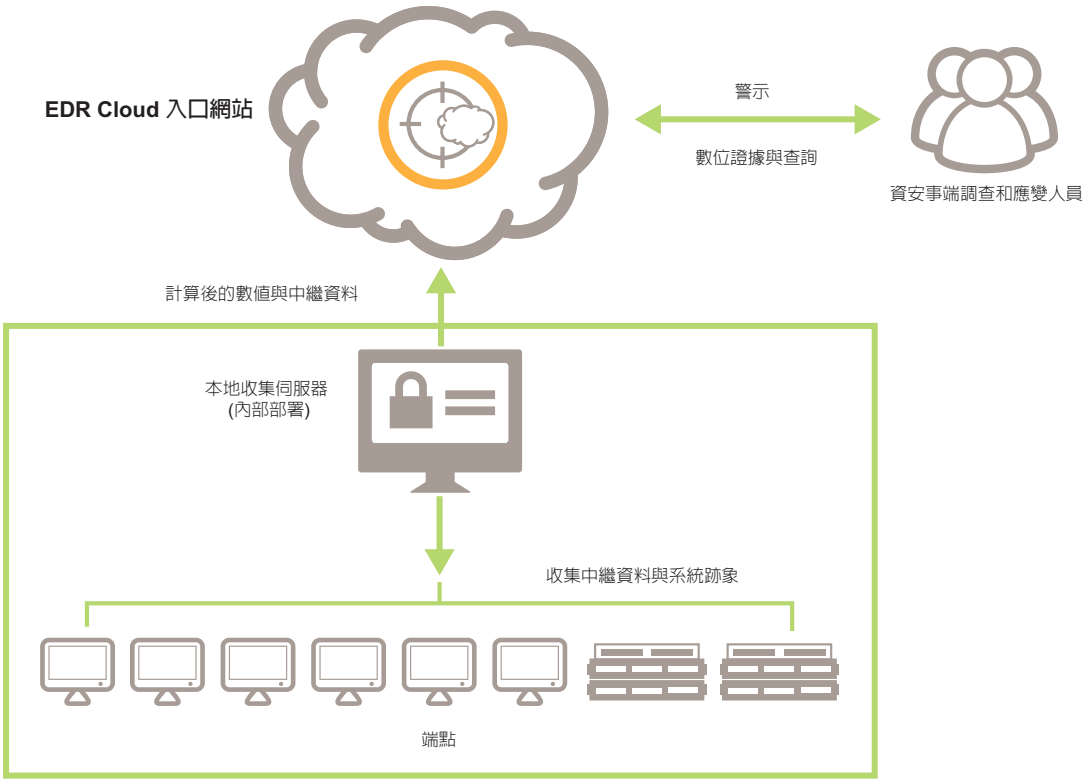


圖 1.賽門鐵克 EDR Cloud 擁有強大的工具，可以將複雜的網路資料視覺化

如何運作

如下面圖表所示，賽門鐵克 EDR Cloud 包含一個調查人員入口網站和一個 (或多個) 收集伺服器。入口網站提供了調查人員介面，能執行安全性分析。此款解決方案會從端點收集資料、分析資料用於偵測，並提供工具讓企業進行查詢並修正遭入侵的系統。

Symantec Endpoint Detection and Response Cloud (EDR Cloud)



內部部署的伺服器會持續從電腦蒐集重要的鑑識資料。收集來的資料包括了未知檔案、程序中繼資料、程式、服務、模組、檔案、自動執行項目、使用者行為、網路連線和時間表。資料收集是被動式行為，在 60 秒內結束，且對一般使用者體驗不會有任何影響。

規定

瀏覽器使用者介面需求

2.9 版需要 Silverlight 以及 Microsoft Internet Explorer 11 或更新版本

3.0 版支援 Mozilla Firefox 26 或更新版本和 Google Chrome 32 或更新版本

收集伺服器需求 (資料保存庫)

透過 Windows Server 2016 執行的 Windows 7

支援 VMware、HyperV 虛擬機器

端點需求

Windows XP 及更新版本

macOS Sierra、El Capitan、Yosemite

Redhat Linux 7.0 及更新版本，32 位元和 64 位元版本

CentOS、Mint、Cinnamon、32 位元和 64 位元版本

參考資料:

1. 第 22 期賽門鐵克網路安全威脅研究報告22

關於賽門鐵克

賽門鐵克公司 (NASDAQ：SYMC) 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。同樣地，全球各地超過 5,000 萬的人們和家庭社群，也仰賴賽門鐵克的諾頓產品和 LifeLock 產品套裝軟體來保護自身的居家數位生活及各種裝置。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 www.symantec.com.tw。

台灣賽門鐵克股份有限公司 | 地址：台北市信義路五段 7 號台北 101 大樓 13 樓 A 室 |
電話：(02) 8726-2000 | 傳真：(02) 8726-2199 | www.symantec.com.tw

SYMC-DS-EDR_Cloud-TW-v1-bb