白皮書：
SYMANTEC™ ADVANCED THREAT PROTECTION

Symantec Advanced Threat Protection

利用 Symantec Synapse™ 加速資安事端應變

本文件的目標讀者群

閱讀以探索 Symantec Synapse 如何提供強化的資安事端應變與工作流程，以便透過整合與交叉比對端點、網路及電子郵件的方式，降低誤報並排定安全事件的優先順序。

Symantec

內容

概述

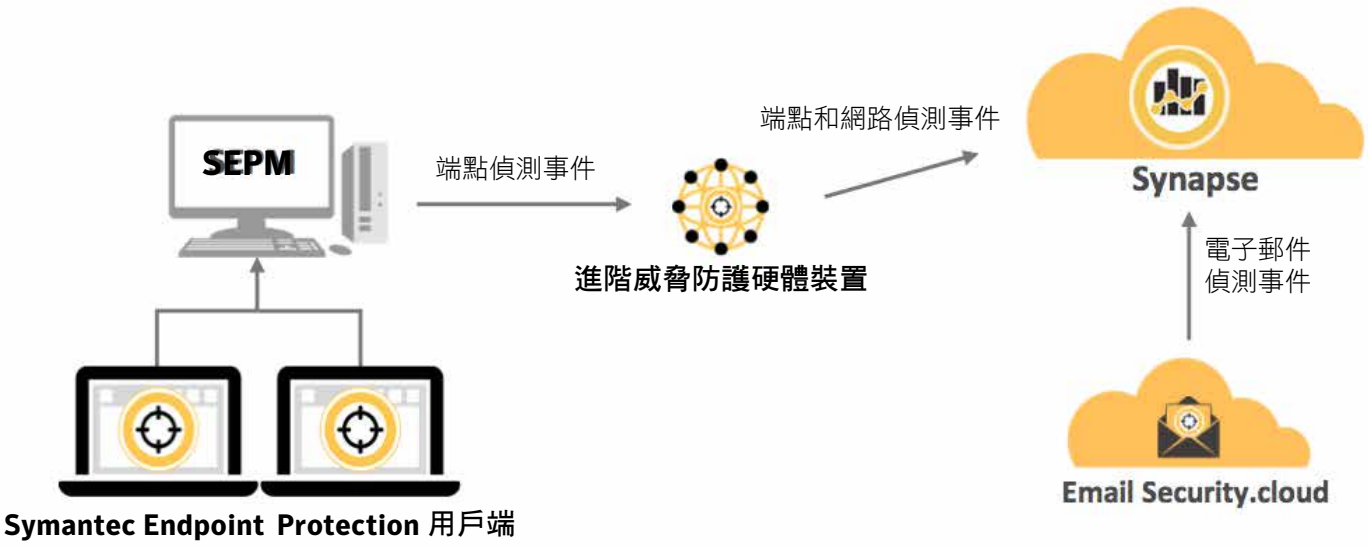
Symantec Synapse 是 Symantec Advanced Threat Protection 隨附的最新技術，它能整合並交叉比對 Symantec™ Endpoint Protection、Symantec™ Email Security.cloud 及 Symantec Advanced Threat Protection: Network 硬體裝置的安全事件資料，協助企業辨識應優先回應的資安事端，以及已遭現有安全控管攔截的資安事端。此舉能夠大幅減少安全分析師需要調查的資安事端數量，使分析師得以「密切注意」最重要的事件。有了 Symantec Synapse，Symantec Advanced Threat Protection 便可在安裝及設定後開始匯入、搜尋及交叉比對所有控制點的資料，而且不到一小時即可完成。

Synapse 可檢驗一些由威脅防護和威脅偵測應用程式產生的安全事件屬性 ，供日後進行交叉比對。當指定的網路或電子郵件事件 (含酬載端點區塊) 結案，及/或其他事件具有一或多個下列相同屬性時，便會交叉比對這些事件：

- **網址/外部 IP 位址** – 列出事件中涉及相同外部網址的資安事端。
- **內部 IP 位址** – 顯示相同內部電腦偵測到的資安事端。
- **檔案雜湊 (SHA256)** – 顯示下載相同檔案的資安事端。
- **VANTAGE 特徵** – 列出因偵測到相同行為特性而經 Symantec Vantage 入侵防護技術判定的資安事端。
- **AV 特徵** – 列出由相同 Symantec Antivirus 特徵所判定的資安事端。

持續檢查相關屬性和交叉比對事件的程序相當耗費資源，因此我們仰賴 Synapse 雲端平台來執行計算工作的重要部分，以維護各企業所有資安事件之間的關係。如此可協助降低內部硬體需求，並確保 Symantec Advanced Threat Protection 能夠迅速找出可能規避偵測的攻擊。

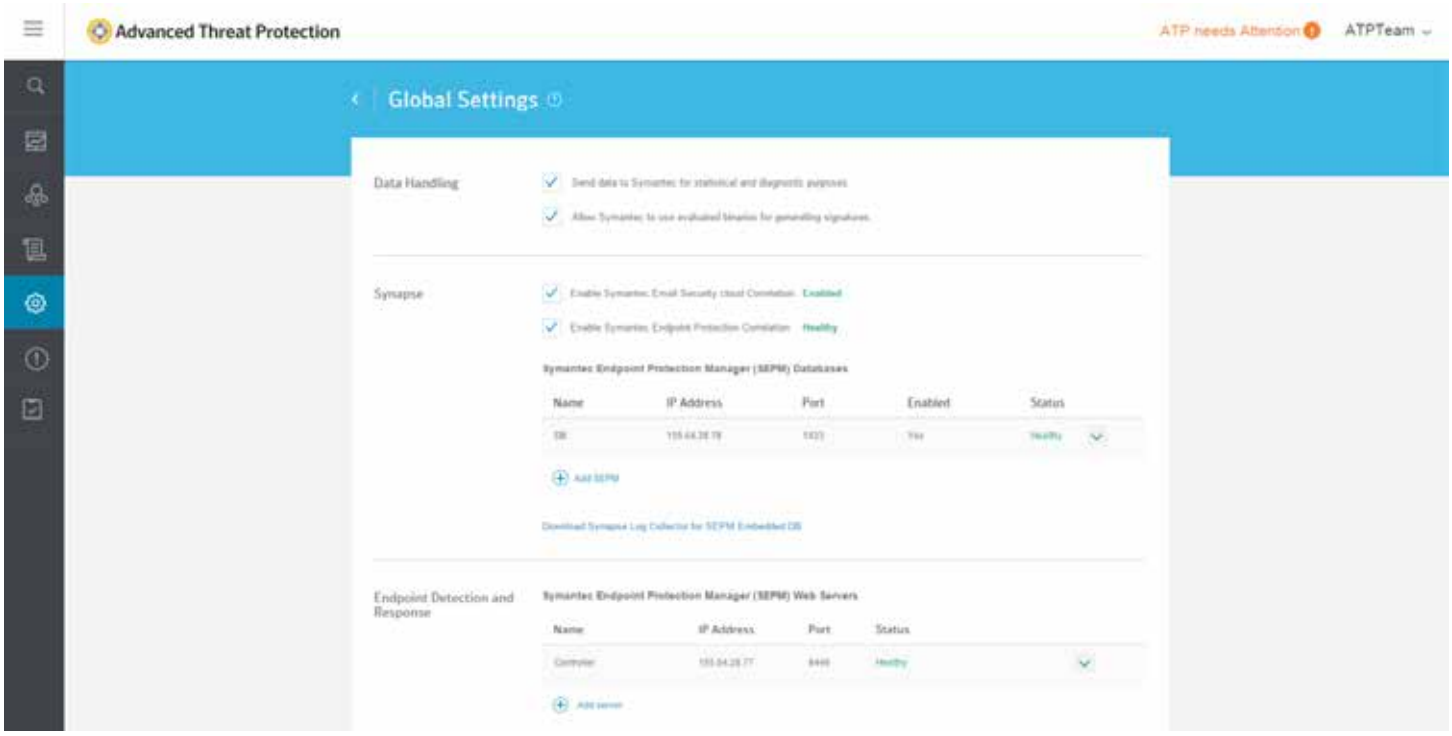
使用 Symantec Synapse 時，Symantec Advanced Threat Protection 主控台能夠在單一位置提供客戶瞭解攻擊所需的所有資料，完全不必手動搜尋。



設定 Symantec Synapse

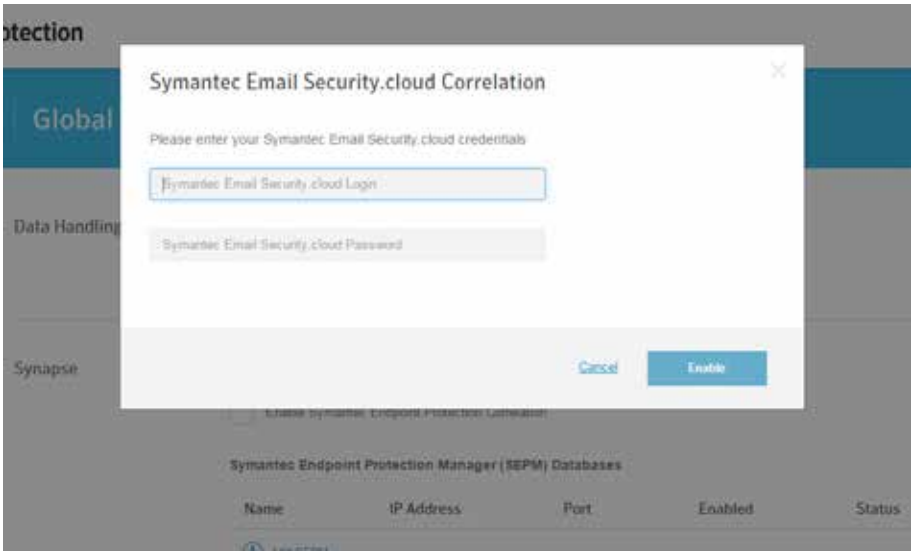
Synapse 經過精心設計，因此設定程序相當簡單。若要交叉比對端點事件與網路和電子郵件偵測，需要提供下列三項資訊：

- 可存取 Symantec Endpoint Protection Manager (SEPM) 伺服器的帳戶憑證。
- 指定 SEPM 使用的資料庫類型 - 內嵌式資料庫或 Microsoft SQL Server。
- 指派給 SEPM 伺服器的 IP 位址。



完成設定程序後，Synapse 會開始擷取在 SEPM 的活動訊號集中包含的端點判定資訊。這些端點事件會連同所有其他 Advanced Threat Protection: Network 事件一併收集，並提供給 Synapse 雲端平台。事件資料會由 Synapse 雲端平台儲存和維護達 90 天。Symantec Endpoint Protection 事件將根據 SEPM 系統管理員設定的 Symantec Endpoint Protection 用戶端活動訊號，開始出現在 Advanced Threat Protection 主控台。這是 Symantec Endpoint Protection 用戶端在 SEPM 伺服器中進行檢查的頻率。預設的活動訊號為 5 分鐘，不過您也可以自行設定；請與您的 Symantec Endpoint Protection 系統管理員討論，以決定用戶端至 SEPM 的更新速率。以近乎即時匯入和交叉比對事件的方式可協助您快速又強大地搜尋整個企業環境。

電子郵件交叉比對的設定更加簡單；使用者只需提供企業的 Symantec Email Security.cloud 系統管理憑證，即可開始進行事件同步程序。這項初始化流程 24 小時內即可完成；不過一旦設定完成，Synapse 每隔五分鐘就會檢查一次變更。



使用案例 1：Synapse 以簡易但強大的搜尋功能提供能見度

有了 Symantec Advanced Threat Protection 的 Synapse 技術，客戶便可建立環境中發生的所有網路、端點及電子郵件判定事件之深入廣泛的安全檢視。此外，Synapse 可以輕鬆簡單地在所有安全事件中搜尋，為關鍵問題快速提供解答。

範例

A 公司的使用者在受到 Symantec Advanced Threat Protection: Network 保護的位置上網。A 公司也訂閱了 Symantec Email Security.cloud 授權，而部分其所屬端點 (非全部) 使用了 Symantec Endpoint Protection。

有三個使用者帳戶收到含惡意網址的電子郵件。此電子郵件經 Email Security.cloud 判定並加以攔截，因此沒有傳送給一般使用者。同一天稍晚，使用者在上班時個人信箱收到一封含有相同惡意網址的電子郵件。由於該電子郵件未遭到攔截，使用者因而造訪了該惡意網址。在網站上，該使用者收到受感染伺服器傳送的酬載。Symantec Advanced Threat Protection: Network 偵測到可疑酬載，並將其送至 Symantec Cynic™ 進行分析。

該檔案已同時傳送到端點。該端點不是由 Symantec Endpoint Protection 管理，因此不會自動判定或攔截。Cynic 傳回此惡意酬載的判定結果，並在 Advanced Threat Protection 中將偵測事件建立為網路事件。A 公司的安全分析師在當天下午檢視偵測事件，也就是一連串活動最初開始後的五小時。 分析師看到 Cynic 的判定後，只要按一下便能迅速在整個環境中開始進行 Synapse 搜尋，以判斷哪個端點擁有此酬載，並依據雜湊和檔案名稱搜尋。

搜尋結果會傳回三個電子郵件判定，其中含有的網址正是檔案下載的來源；還會傳回一個網路事件，其中包含擁有該檔案之未受管理端點的 IP 位址。有了這項情報，安全分析師便可針對下載惡意酬載的特定裝置迅速開始矯正，並且有信心不會再偵測到此攻擊的其他執行個體。

Synapse 將一切安全事件全部整合至單一解決方案，可大幅簡化搜尋並協助應變人員迅速釐清受到偵測事件影響的端點範圍。此外，Synapse 也可根據下列任意一個基本入侵指標 (IOC) 支援完整的環境搜尋：檔案名稱、檔案雜湊、網址 (完整或部分) 及登錄機碼。

使用案例 2：Synapse 可強化環境中的獵捕能力

Synapse 可針對 IOC、甚至賽門鐵克之前未認定或知曉為惡意的檔案強化端點審查。

範例：

聯邦政府機構已就另一家同業公司被特定酬載攻擊得手向您發出警示。攻擊的其中一項 IOC 便是檔案雜湊；您一定會想知道自己的環境中是否存有該雜湊。若要確認，分析師需在搜尋欄位輸入該檔案雜湊，並將「查詢端點」滑桿設為綠色。

Synapse 會查詢端點以及在您環境的 10,000 個端點中尋找，並在 3 個端點中找到該雜湊。此外，這 3 個端點中只有一個擁有關聯的攔截事件。此時，事件遭攔截的端點上無需再執行進一步的動作。但另外兩個端點並未發生攔截事件，因此分析師決定立即隔離這些端點，將其隔絕於環境的其他部分之外。

為了後續追蹤此查詢並結案，分析師會將此檔案雜湊列入黑名單，如此一來，所有本機端點的後續偵測都會遭到攔截。最後，分析師會刪除這兩個隔離端點中的檔案以清理系統，然後再讓這兩個端點重新加入環境中。

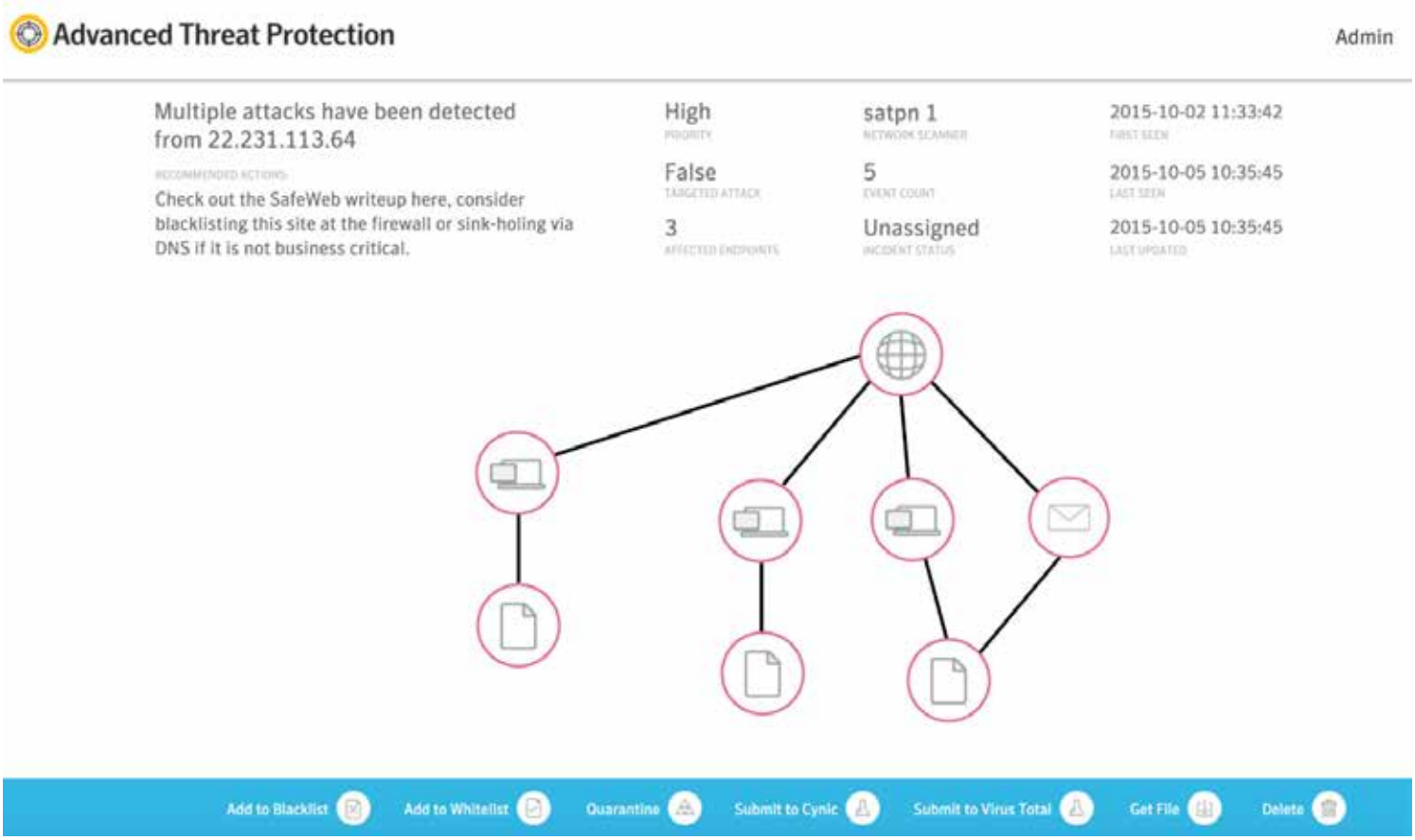
使用案例 3：Synapse 可協助安全分析師有效調查和矯正

Synapse 將所有的 Advanced Threat Protection 偵測器 (包括端點、網路及電子郵件) 的相關事件，交叉比對至需要安全分析人員進一步留意和調查的資安事端。在系統中建立的所有資安事端都是串流規則引擎的結果，也就是邏輯陳述式的集合，可協助 Advanced Threat Protection 瞭解是否有足夠的活動會觸發事件的建立。

範例

我們掌握端點受感染的證明時，就可建立資安事端。所需的證明可以是偵測到受感染網路的流量流向指令和控制伺服器，或是知曉酬載具有惡意且端點無法完整清除其中的所有跡象。這些是已知感染，並且會建立安全分析師必須處理的資安事端。

當我們針對特定且相對較短的時間範圍確認事件活動會連線至原本中立的網域、IP 或網址時，也會額外建立資安事端。這可能涉及相同或多個網路位置、多個檔案下載至單一或多個端點，或是單一或多個端點都遭到指定網域/IP/網址/外部電腦鎖定。決定哪些事件相關聯的情報由 Synapse 掌握，可釐清看似不相干事件之間的關係，並以視覺化方式加以整合，透過如「有機體 (organism)」般靈活的方式，讓您輕鬆簡單地探索、調查資料並進行樞紐分析。



在相同位置提供有機體檢視，讓分析師能夠立即瞭解攻擊範圍並存取各種行動。

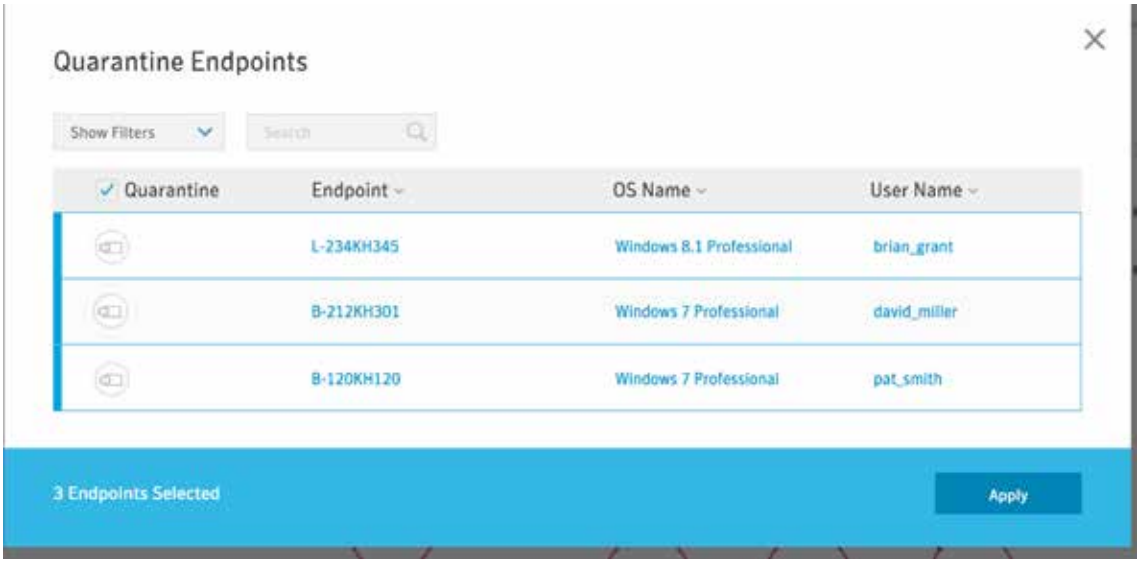
列入黑名單/白名單

在有機體檢視中，安全管理員可迅速簡單地將整個環境中的特定檔案或網路流量屬性立即加入黑名單。Symantec Advanced Threat Protection 可依據 SHA256 和 MD5 檔案雜湊、網址或網域以及 IP 位址或 IP 子網路，將檔案或位置列入黑名單禁止存取。若嘗試存取列入黑名單的檔案或位置將會遭到拒絕，而且也會隨時在 Advanced Threat Protection 主控台上產生偵測事件。

同樣地，安全系統管理員可以將檔案或網路位置列入白名單提供使用者存取，迫使 Advanced Threat Protection 略過偵測引擎並允許自由存取。

隔離端點裝置

按一下有機體檢視中的隔離按鈕即可迅速隔離此資安事端範圍中的裝置。

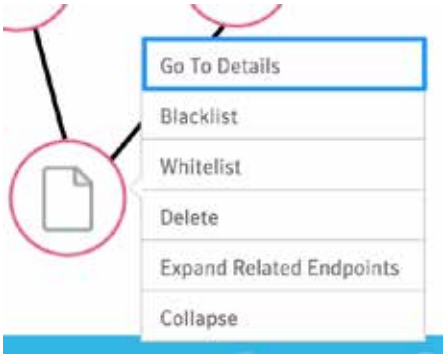


隔離裝置時會使用 Symantec Endpoint Protection 用戶端的網路控制元件，攔截所有網路存取嘗試。隔離的裝置唯一能夠與其通訊的位置是相關聯的 SEPM 伺服器。這樣可避免感染擴散並攔截未經授權嘗試存取網路服務和資料，但安全系統管理員仍可調查和矯正裝置。在調查完成後，可透過相同介面移除隔離，並將完整的網路存取權限還原至裝置。

進一步調查

可疑或經判定的檔案可以傳送到 Symantec Cynic 沙箱做進一步檢查，以提供酬載的實際行為。此外，您只要按一下即可輕鬆查看 Virus Total 和其他安全廠商對於此檔案的瞭解程度。

系統管理員在可疑或已判定之檔案的內容功能表中，查看 Symantec Advanced Threat Protection 掌握的所有情報。



本機內容提供的方式為此檔案在環境中查看的次數、首次查看時間、偵測到的地點以及檔案來源。

Symantec Cynic 沙箱分析的輸出內容會詳述檔案在裝置中啟用時採取的行為和動作，以及檔案程序嘗試進行通訊的任何位置和目的地。這些入侵指標可用來搜尋環境中其他感染證明，有可能是鎖定範圍更廣的目標攻擊活動的一部分。

Cynic Observed File, Registry, System Changes

Severity	Type	Description	PID
1	Process Started	C:\Windows\SysWOW64\cscript.exe	2940
1	Process created by	C	2940
1	Opened a registry key	HKEY_CURRENT_USERS\Software\Microsoft\Windows Script Host\Settings	2940
1	Created window	0	2940
1	Opened a registry key	HKEY_CLASSES_ROOT\.js	2940

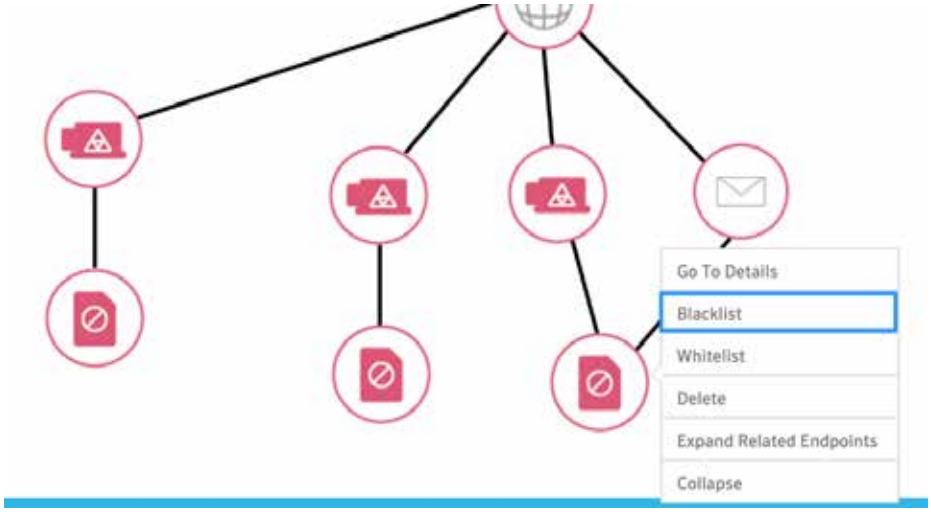
15 Total

Cynic Observed Network Analysis

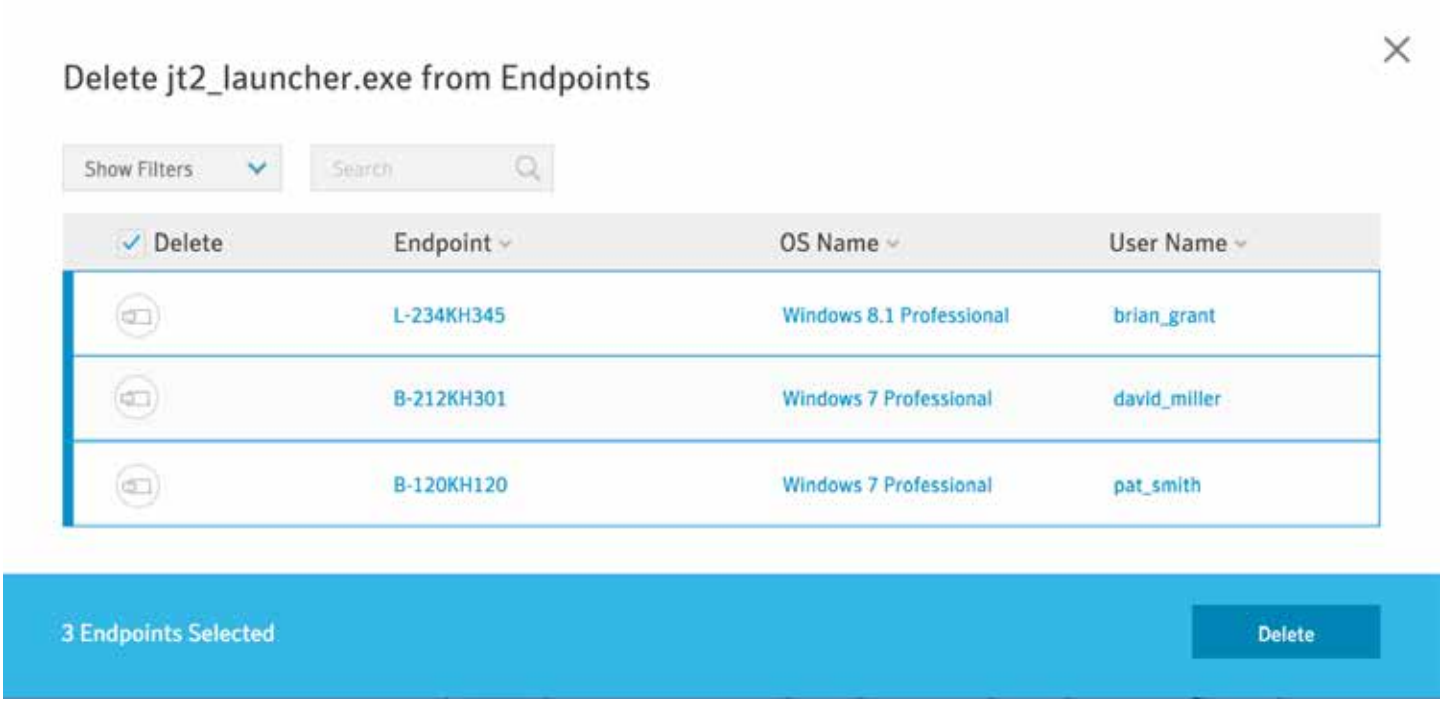
Domain/IP	Protocol	Port	URL
router.bittorrent.com	DNS	--	--

單鍵矯正

調查完成後，Symantec Synapse 便可極為輕鬆地進行矯正。現在已經明確掌握哪部電腦含有檔案，便可利用 Symantec Endpoint Protection 用戶端移除檔案，避免進一步感染。安全分析師可重複使用內容功能表，自動將檔案資訊新增至黑名單。



在檔案列入黑名單後，選擇「刪除」將會移除該檔案以及這次資安事端範圍中所有端點的任何相關跡象。



總結

企業可打造專屬平台進行資料共用和情報交叉比對、使用安全資訊與事件管理 (SIEM) 平台，以及寫入記錄檔剖析器與收集器將資料汲取至單一位置；對於某些安全企業來說，這是相當明智的作法。然而，寫入和調整政策以精確偵測攻擊和誤報之間的差異所需的作業，以及管理、維持和更新這類環境的營運需求，對於絕大多數的企業來說並不可行，尤其是發現攻擊時所考量到矯正的時間與成本。

有了 Symantec Advanced Threat Protection，Synapse 就能彙總所有控制點的情報，大幅降低安全分析師需要調查的資安事端數量，還能自動為遭入侵且需立即矯正的系統排定優先順序。還能提供客戶必須知悉的所有資料，使其得以瞭解某個位置的攻擊情況，完全不需要人工搜尋，而且還結合全球規模最大的網路情報網路所提供的全球遙測資訊，以及各地客戶端點、網路及電子郵件的環境，以找出規避偵測的各種攻擊。

運用目前安裝的 Symantec Endpoint Protection 及 Symantec Email Security.cloud，Symantec Advanced Threat Protection 便可提供安全分析師提升工作效率和做出明智決策所需的能見度，包括透過單一主控台進行單鍵矯正以及獵捕所有端點的入侵指標，完全不必安裝任何全新的端點代理程式。

關於賽門鐵克

賽門鐵克公司 (NASDAQ：SYMC) 是網路安全領域的全球領導廠商。我們運行全球規模最大的網路情報網之一，因而得以發現更多線上威脅，並保護更多客戶免於遭受新一代網路攻擊。無論最重要的資料存放於何處，我們都能協助公司、政府機構和個人妥善保存。

如需任何分公司和聯絡電話的相關資訊，請造訪我們的網站。

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/zh/tw