Check Point SandBlast Agent

Check Point SandBlast Agent

提供保護的能力。
可以了解的深入見解。

產品優勢

- 簡單且非侵入式的解決方案，並提供直覺的使用者介面
- 主動阻擋新的和未知的惡意軟體，避免它們接觸端點
- 主動提供下載檔案的安全版本給使用者，以維持業務的工作效率
- 即時阻擋網路釣魚攻擊來保護使用者憑證
- 在探索前就提供攻擊歷史事件的全面檢視
- 充分了解根本原因、惡意軟體進入點，以及損害範圍
- 加速回應時間，減少再次感染的機會

產品功能

- 防範多種攻擊管道，包括網頁下載、外部儲存設備、橫向移動或經過加密的內容
- Threat Extraction 可使用安全元素重新建構入埠的檔案
- 找出和遏止被感染的主機以控制損害和惡意軟體的擴散程度
- 使用動態分析和啟發式功能阻擋詐騙的網路釣魚網站
- 自動建立包含主要攻擊資訊的可執行鑑識報告
- 當使用者試圖在外部網站使用公司密碼時會發出警示，以確保憑證的安全

深入見解

精密的社交工程和以網頁為基礎的惡意軟體攻擊使得資安事件頻傳，網頁瀏覽器普遍成為威脅入侵端點裝置的一個進入點。惡意軟體會躲藏在網頁下載內容或網頁郵件的附件中。您的員工可能會在無意間成為網路釣魚和社交工程的受害者，因為即使只是他們在非公司網頁服務上重複使用公司憑證和密碼，都會讓公司處於風險之中。換言之，使用者需要即時的安全防護措施，以便支援他們能不受限制地利用網際網路立即傳送關鍵性檔案和電子郵件。

此外，隨著越來越多員工使用企業裝置在遠端進行工作，以及員工、約聘人員和顧問將各種系統攜入企業，網路犯罪分子可以鎖定傳統端點安全保護的弱點來滲透和感染這些工作人員的系統。一旦入侵成功後，駭客就會利用橫向通訊穿越網路，感染其他裝置。隨著威脅不斷演變，企業必須找到一個方式來偵測、防禦和快速回應端點遭受的攻擊，以便控制損害。

您應該如何保護員工免於這些新興威脅的干擾，同時讓他們可以依照業務需求的步伐完成工作？

我們的解決方案

Check Point SandBlast Agent 可將領先業界的網路保護擴展到端點裝置，包括 SandBlast Zero-Day Protection 對網頁瀏覽器和端點裝置的進階保護能力。這個產品可以完全即時防範各種威脅管道，讓您的員工無論身在何處都可以安全地工作，而且不會影響工作效率。SandBlast Agent 會防範經由網路下載的威脅、由卸除式儲存裝置複製的內容，電子郵件中的連結或附件、在網段內各系統之間橫向移動的資料和惡意軟體，以及透過加密內容傳入的有毒檔案。

SandBlast Agent 使用零網路釣魚 (Zero Phishing) 技術，能主動阻擋瀏覽新的和未知的詐騙網站的行為，並防止公司密碼遭到濫用，以保護使用者的憑證。

SandBlast Agent 會持續收集所有相關系統事件以擷取鑑識資料，然後提供可執行的事件分析以快速了解完整的攻擊週期。在取得範圍、損害和攻擊管道的可見度後，事件回應團隊可以完全發揮產能，並且將企業暴露的情形減至最小。

防範零時差惡意軟體

Check Point SandBlast Agent 可將 SandBlast Zero-Day Protection 經過實證的保護擴展到端點裝置與網頁瀏覽器。Threat Extraction 會在瞬間重新建構下載的檔案，避免可能的威脅，並且及時提供一份安全版本給使用者。同時，Threat Emulation 會快速檢測虛擬沙箱中的檔案，找出惡意行為並阻擋新的惡意軟體和目標式攻擊的感染。

阻擋零時差網路釣魚攻擊

SandBlast Agent 的零網路釣魚功能使用動態分析和進階的啟發式功能，可以即時識別並阻擋在使用者瀏覽新的和未知的網路釣魚網站時，惡意軟體經由網頁瀏覽器鎖定使用者憑證的行為。

此外，這項功能還能在使用者違反公司密碼重複使用政策時發出警示，避免使用者在瀏覽第三方網站時因密碼外洩而導致企業憑證遭竊的情形。

找出和遏止感染

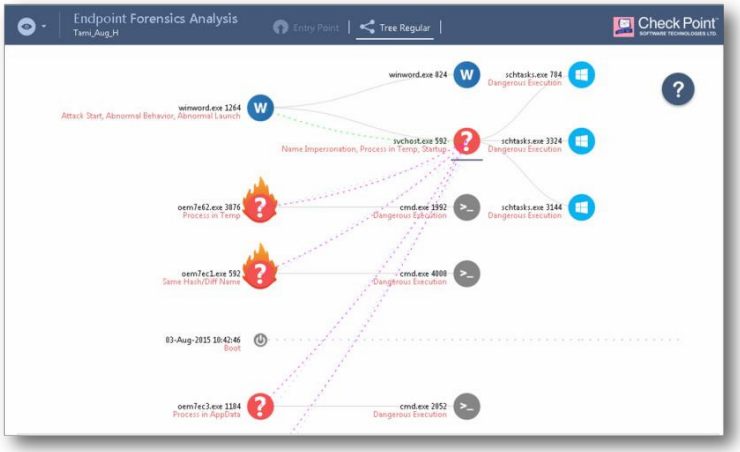
使用本機版本的 Anti-Bot 安全保護，並透過 ThreatCloud 持續更新最新的威脅情報，SandBlast Agent 可識別並阻擋殭屍程式和指揮與控制伺服器之間的通訊，並且隔離任何已經被感染的主機。

涵蓋各種威脅管道的全方位保護

SandBlast Agent 會協助使用者防範利用網路釣魚手法進行網路下載的威脅、由卸除式儲存裝置複製的內容，電子郵件中的連結或附件、在網段內各系統之間橫向移動的資料和惡意軟體所造成的感染，以及透過加密內容傳入的有毒檔案。

安全事件的完全可見度

Check Point SandBlast Agent 的鑑識能力提供完全可見性，可以監控和記錄所有端點事件：受影響檔案、啟動程序、系統登錄檔變更，以及網路活動。SandBlast Agent 可以追蹤並回報惡意軟體採用的步驟，包括零時差威脅。藉由 SandBlast Agent 的持續監控，可確保資料在遭受攻擊後仍然可用，甚至是那些會移除檔案和其他系統受駭指標的攻擊。



可執行的事件分析

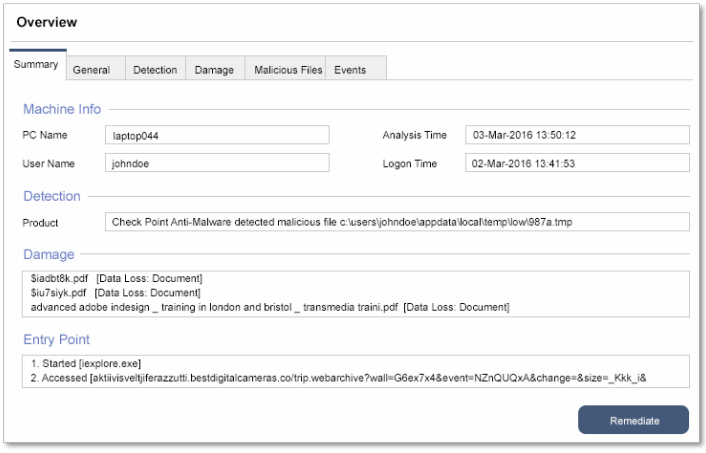
惡意事件發生時，會自動啟動鑑識分析程序。其結合使用一個先進的演算法和原始鑑識資料的深入分析，可以製作出一份全方面的事件摘要。該摘要會提供主要的可執行攻擊資訊，包括：

惡意事件—在整個攻擊週期中，有哪些可疑行為的證據被偵測到？

進入點—攻擊如何進入網路？用於攻擊的主要元素在什麼地方？攻擊如何發動？

損害範圍—惡意軟體作用後對業務會發生什麼影響？哪些資料遭駭和/或複製到企業外部？

受感染主機—還有誰或什麼設備受到影響？



這種全方面的攻擊診斷和可見性可以支援修補作業。系統管理員和事件回應團隊可以迅速而有效地分流和解決攻擊，讓企業可以比尋常還快地恢復運作。

詳細的事件報告

SandBlast Agent 內建的鑑識能力可讓您使用 SmartEvent 由一個中央位置檢視被閘道或端點本身觸發事件的報告。安全管理員也可以產生已知惡意事件的報告，提供一個詳細的網路獵殺鏈分析。這些報告提供可執行的事件分析，可加速了解整體攻擊週期的程序、損害和攻擊管道。

第三方整合

SandBlast Agent 可和 Antivirus 與其他 Check Point 安全解決方案一起運作，也能和其他廠商的產品整合。其可以增強現有 Antivirus 產品的偵測能力，提供防禦進階型威脅的能力並提供可執行的事件分析。當因事件、其他 Check Point 元件或第三方解決方案觸發 SandBlast Agent 時，其會分析端點鑑識日誌並產生 SmartEvent 和 SmartLog 中可以觀看的報告。

SandBlast 解決方案系列

SandBlast Zero-Day Protection 解決方案還包括其他產品，可以為網頁瀏覽器、端點和雲端應用程式提供進階型威脅防護。

易於部署與管理

SandBlast Agent 提供彈性的部署選項，可以符合所有企業的安全需求。適用於瀏覽器的 SandBlast Agent 可以 SandBlast Agent 的一個整合的部分快速部署到端點上，或是以佔用空間最少的獨立解決方案使用在網頁瀏覽器。

這個非入侵性、低耗能的部署使用 SandBlast 遠端沙箱服務 (無論是 SandBlast Service 或您自有的私人設備)，對本地效能的影響可降至最低，並且完全相容已經部署的應用程式。

適用於瀏覽器的 SandBlast Agent 套件

適用於瀏覽器的 SandBlast Agent (SandBlast Agent for Browsers) 是瀏覽器擴充元件，專門防範使用網頁瀏覽器當成主要進入點的攻擊。其包含 Threat Extraction、Threat Extraction、零網路釣魚和憑證保護的能力。

這個獨立式解決方案可以簡單的網路瀏覽器擴充元件實作，對希望快速部署且佔用空間小的企業是最好的選擇。適用於瀏覽器的 SandBlast Agent 使用標準端點管理工具，如 GPO (群組政策物件)，以便將政策推送到使用者端點。

SandBlast Agent 完整套件

SandBlast Agent 可防範端點裝置上的威脅。其包含 Threat Extraction、Threat Extraction、鑑識、防殭屍程式的能力，以及零網路釣魚和憑證保護。

您可以快速部署 SandBlast Agent，並由 SmartCenter 集中管理所有政策。而且您可以經由 SmartEvent 和 SmartLog 存取事件日誌和事件報告，深入了解即使是最進階的攻擊。

技術規格

SandBlast Agent - 套件	
可用的部署套件	• 獨立套件 - **SandBlast Agent for Browsers**，包含 Threat Extraction、Threat Extraction、零網路釣魚和憑證保護的能力 • 完整套件 - **SandBlast Agent Complete**，包含所有 SandBlast Agent for Browsers 的功能，再加上防殭屍程式、鑑識和自動事件分析 • 完全端點保護套件 - **Endpoint Suite**。SandBlast Agent 完整套件再加上全磁碟加密和防毒
端點安全 - SandBlast Agent	
作業系統	• Windows 7、8 和 10 • Windows Server 2008 和以上版本
瀏覽器保護 - 適用於瀏覽器的 SandBlast Agent	
支援的平台	• Google Chrome • Internet Explorer (即將推出)
下載保護 - Threat Emulation 和 Threat Extraction	
支援的檔案類型 - Threat Extraction	• Adobe PDF • Microsoft Word、Excel 和 PowerPoint
支援的檔案類型 - Threat Emulation	• 超過 40 種檔案類型，包括：Adobe PDF、Microsoft Word、Excel、PowerPoint、執行檔 (EXE、COM、SCR)、SWF、RTF 和封存
Threat Emulation 和 Threat Extraction 部署選項：	• SandBlast Service (託管在 Check Point 雲端) • SandBlast 設備 (託管在內部)
零網路釣魚和憑證保護	
零網路釣魚	• 即時防範未知的網路釣魚網站 • 透過靜態和啟發式偵測索取使用者憑證的網站的可疑元素
企業憑證保護	• 偵測在外部網站重複使用企業憑證的行為
檔案系統監控	
Threat Emulation	• 由卸除式儲存裝置複製的內容 • 在網段內各系統之間橫向移動的資料和惡意軟體
實施模式	• 偵測和警示 • 阻擋 (背景與保留模式)
防殭屍程式	
實施模式	• 偵測和警示 • 阻擋 (背景與保留模式)
鑑識	
分析觸發器	• 在網路或端點進行防殭屍程式偵測 • 在網路進行 Threat Emulation 偵測 • 在端點使用 Check Point Antivirus 進行偵測 • 在端點使用第三方防毒進行偵測 • 入侵指標 (IoC)
損害偵測	• 自動識別：資料擴散、資料竄改或加密、金鑰側錄
根本原因分析	• 即時追蹤和分析跨多系統重新啟動的根本原因
惡意軟體流分析	• 自動產生攻擊流的互動式圖形化模型
惡意行為偵測	• 超過 40 種惡意行為類別 • 數百種惡意指標
管理	
政策管理	• 端點政策管理 (EPM)
事件監控	• SmartLog • SmartEvent
端點管理版本	• E77.30.02 和以上版本
端點管理 - 可用套件	• 預設包含 SmartCenter 和 Smart-1 設備中 • 可以軟體授權取得

聯絡我們

全球總部 | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | 電話：972-3-753-4555 | 傳真：972-3-624-1100 | 電子郵件：info@checkpoint.com
台灣分公司 | 6F, No. 6 Sec.4 Xinyi Rd., Da'an Dist., Taipei City 106, Taiwan (ROC) | 電話：886-2-2703-2798 | 傳真：886-2-2703-2796 | www.checkpoint.com