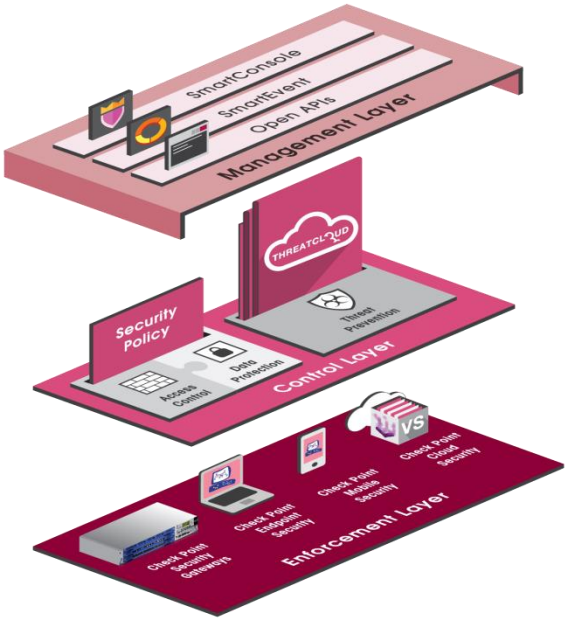
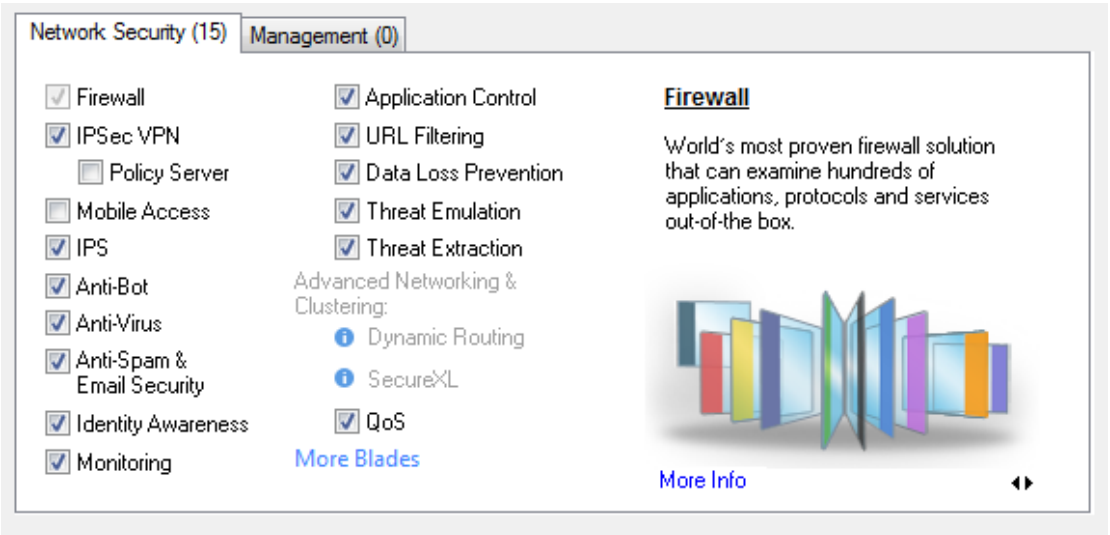
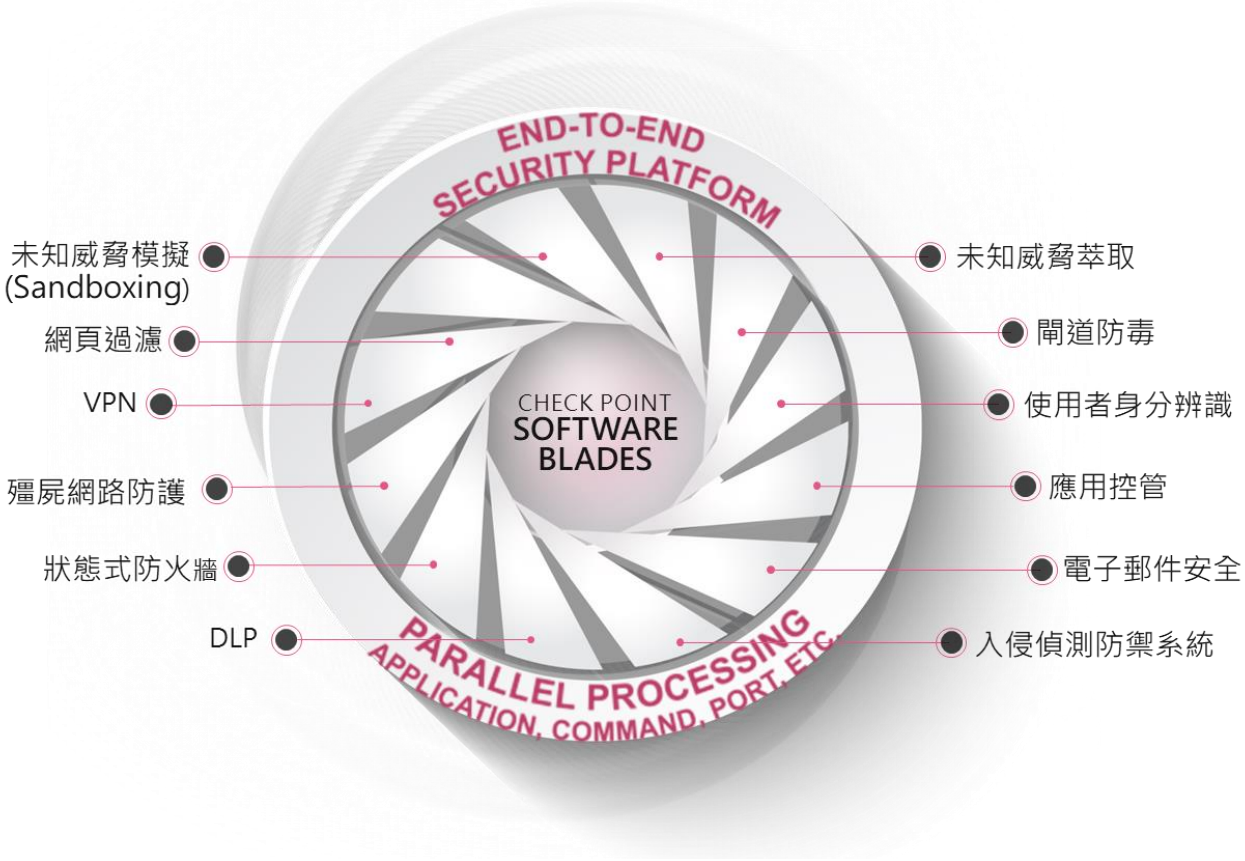
Check Point 軟體安全公司(www.checkpoint.com)是全球首屈一指的資訊安全供應商。其獨特技術提供客戶頂級資安威脅防護，並可大幅降低企業總成本。Check Point 以其軟體刀鋒架構(Software Blade Architecture)為基礎，持續研發領先防護措施，提供客戶彈性且簡易的解決方案，可完全客製化以符合任何企業或環境實際上的安全需求。Check Point 是唯一超越技術層面的資安供應商，將安全防護轉為商業流程。財星雜誌前100 大企業以及全球成千上萬各種規模的公司均是 Check Point 的客戶，除了客戶的肯定，Check Point 更是已經連續 20 年在 Garter 的企業等級防火牆中，被評鑑為領導廠牌。



Check Point 獨特的 SDP(Software Define Protection)將繁雜的防火牆管理及部署整合成簡易的三層次架構，藉由分層分工架構，協助使用者方便管理並且維持高可視性，資安威脅一手掌握。



Check Point軟體刀鋒(Software Blade)介紹



Check Point 軟體刀鋒架構 (Software Blade Architecture)是第一個，也是唯一一個可提供完整、彈性和可管理的安全性給所有企業的安全性架構。所有組織都可以透過這個架構容易且有效地量身建立適用的安全性基礎結構，以符合重要和目標性的商業需求。甚至，當新威脅和緊急需求出現時，Check Point 軟體刀鋒架構 還能依需要快速、彈性地擴充安全性，無需額外的硬體或管理複雜性。所有解決方案都可以透過單一主控平台集中管理，以降低複雜性和營運的負擔。Check Point 軟體刀鋒提供較低的總持有成本 (TCO)、更快速的投資報酬率 (ROI)，以及具效益的保護，可以符合現在或未來任何網路或端點安全性的需求。而其獨立、模組化和集中管理的特色，能讓組織根據適當的保護和投資平衡自訂安全性組態。您只要點按滑鼠，就能在任何閘道或管理系統上快速啟用和設定軟體刀鋒，不需要硬體、韌體或驅動程式升級。而且，隨著需求演變，您可以容易地啟用額外的軟體刀鋒，在現有組態上擴充安全性。

IPS軟體刀鋒

Check Point 的 IPS 軟體刀鋒提供整合性次一代防火牆入侵防禦功能，提供全面的威脅覆蓋，包含了用戶端，主機端，作業系統和其他漏洞，惡意軟體/蠕蟲感染等等。IPS 軟體刀鋒功能的多層威脅檢測引擎結合了特徵碼、協議驗證、異常檢測，行為分析和其他方法，提供最高水準的網路 IPS 保護。IPS 掃描引擎能檢查相關性的攻擊，無須深度檢測即可快速過濾 90%的流量，進而減少維運成本並提高阻擋的準確性。

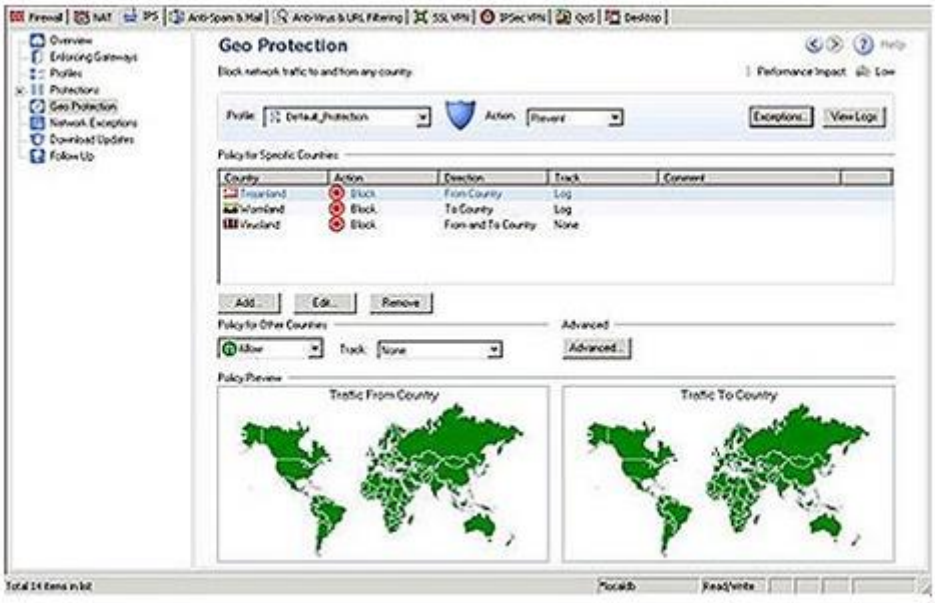
主要優點

完整功能的 IPS

提供完整功能防護，可針對惡意軟體、DoS/DDoS 攻擊、應用程式與 OS 弱點等完整防護。

方便設定的地理保護機制

提供地理保護機制，可監控網路流量的來源與目的地國家，並可創造例外情況的政策允許合法的流量通過，同時封鎖或監控未知或不信任來源流量。

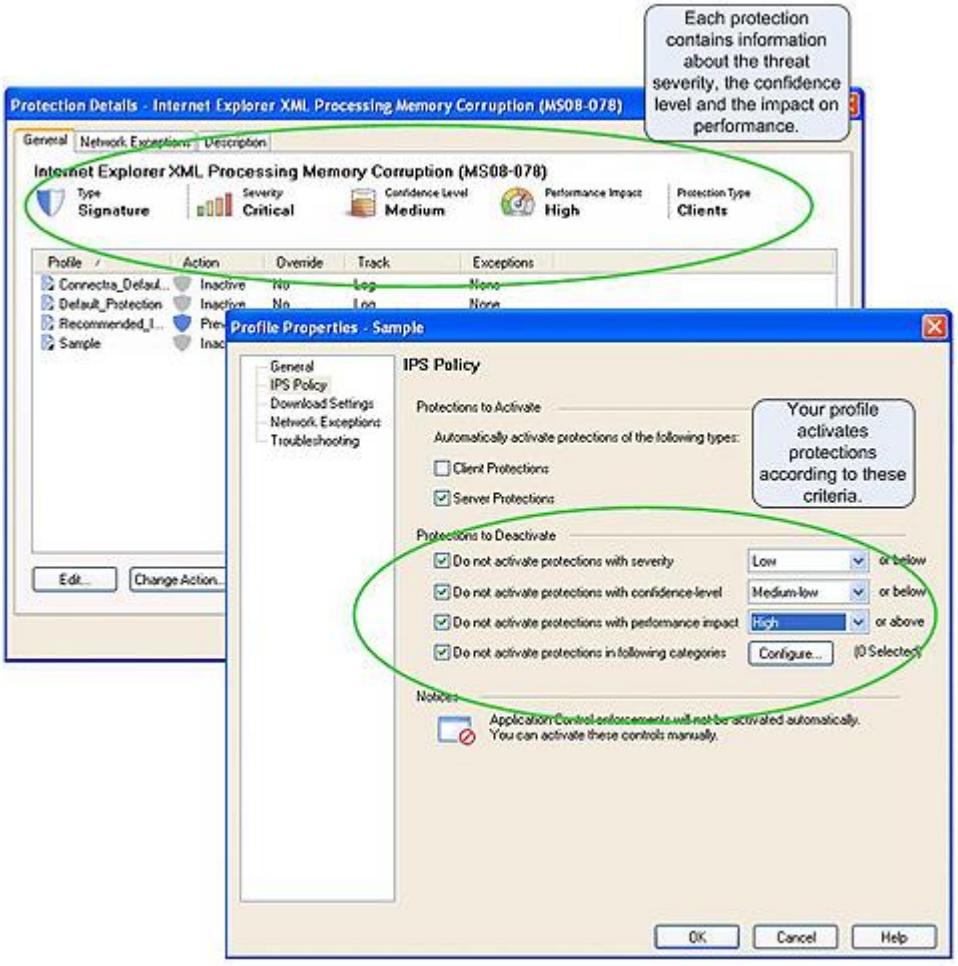


無痛的部署方式

整合於 Open server，無須新增硬體，即可在現有防火牆上開啟，並可設定偵測模式，確保現有流量不受影響。

動態的威脅管理

整合 Check Point 事件管理軟體刀鋒 SmartEvent，使用者可於事件管理介面上直接進行管理規則調整。另外，使用者可自訂特徵碼防禦更新規則，在 IPS 更新特徵碼時，自動套用規則，既能提升防護效能又無須增加維運成本。



可檢查 **HTTPS** 加密內容

可針對 HTTPS 內容加以解析，並可設定 Bypass 規則，針對特定種類網頁不進行解析，保護使用者隱私。

單一整合的管理/報表介面

整合 Check Point 既有管理與報表介面，在單一平台上即可進行多項軟體刀鋒功能設定與報表檢視，大幅降低維運成本。

App Control軟體刀鋒

應用程式偵測和使用控制

啟用安全政策可以識別、允許、阻擋或限制數千種應用程式的使用，不論其通訊埠、通訊協定，或是在網路中穿梭的躲避技巧為何。和身分識別感知能力結合之後，可以制定非常精細的政策定義。其可以根據使用者或群組的需求，以及應用程式在安全、產能和資源使用方面的特性來管制使用者和群組可以如何使用應用程式。可以直接從防火牆容易地對每一個使用者或群組定義以應用程式為基礎的政策。

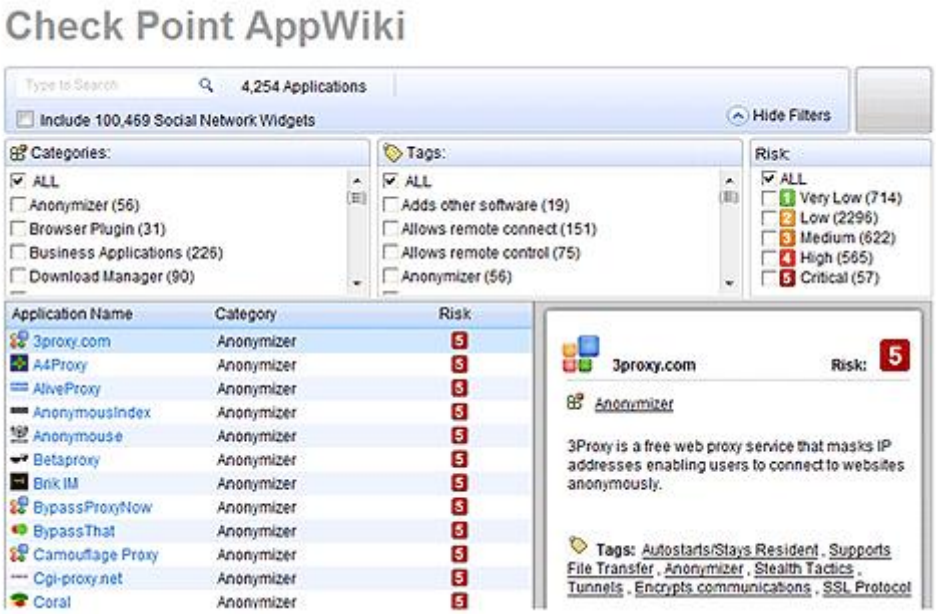
主要優點

精細的應用程式控制

識別、允許、阻擋或限制對數千種應用程式的使用，不論其通訊埠或通訊協定為何，以防範來自網際網路應用程式且不斷增加的威脅媒介。

採用最大型的應用程式檔案庫 **AppWiki**

全方位的應用程式控制採用了業界最大型的應用程式檔案庫，能掃描和偵測過 7,800 種不同的應用程式和超過 264,000 個 Web 2.0 的 Widget。



創新的 **UserCheck**

UserCheck 技術會即時向使用者詢問並提供關於 Web 2.0 的風險、原則和使用方式，簡化應用程式控制的作業。

整合到所有安全性閘道

可以在任何 Check Point 安全性閘道啟用應用程式控制。

集中式管理

啟用可以從單一個簡單易用的主控台中集中管理的政策，以簡化管理作業。

使用者和電腦感知能力

身分識別感知能力能啟用政策定義，根據使用者、群組、內容或頻寬來部署特定的安全政策。這項功能提供企業管制網際網路應用程式使用的能力，以在安全性和商業需求之間取得平衡。
藉由採用無縫和無代理程式的方式與 Active Directory 整合，可以提供完全的使用者識別，以便直接從防火牆根據使用者或群組簡單制定應用程式的政策定義。可以透過以下三個簡單的方法之一取得使用者的識別資訊：

查詢 Active Directory

透過管制的入口網站

安裝一個單次式、精簡型用戶端上的代理程式

Antivirus軟體刀鋒

Check Point Antivirus 軟體刀鋒能保護您的邊界，阻擋數量越來越多的威脅。Antivirus 軟體刀鋒使用最大型雲端即時即時安全威脅知識庫 ThreatCloud™ 持續更新的防毒特徵(病毒碼) 和異常式防護，能在閘道處偵測和阻擋惡意軟體，避免它們影響使用者。

我們的解決方案

Check Point 的威脅防禦解決方案包含 Antivirus 軟體刀鋒和來自 ThreatCloud™ 的支援，能提供時刻更新的安全情報給安全閘道，包含超過 2 億 5 千萬個位址的殭屍程式探索結果、超過 480 萬個惡意軟體特徵和超過 30 萬個遭到惡意軟體感染的網站。
ThreatCloud 的知識庫會彙整來自全球閘道的攻擊資訊而不斷更新，還會接收來自全球威脅感應器的饋入資訊，以及 Check Point 研究實驗室和業界最佳惡意軟體研究成果的情報。經過彙整的安全威脅資訊會分享給所有閘道使用。
由 ThreatCloud™ 所支援 ThreatCloud 是第一個對抗電腦犯罪的協同網絡，會提供即時安全情報給安全閘道軟體刀鋒：

分析超過 2 億 5 千萬個位址以找出殭屍程式

480 萬個惡意軟體特徵

30 萬個惡意網站

完全的防毒解決方案

在單一閘道上的整合式威脅防禦

時時更新的防護，可防範傳入的惡意檔案

可和 Anti-Bot 軟體刀鋒整合，提供統一的防護和管理

可以部署在所有閘道上

從一個使用者容易操作的主控台集中管理

優勢

閘道阻擋惡意軟體，避免它們造成損害

使用 ThreatCloud 的即時威脅情報對抗不斷變動的威脅情勢

在受保護的環境中分析可疑檔案，以識別出未知的惡意軟體

利用整合式的威脅報告和儀表板觀看和管理威脅

阻擋傳入的惡意檔案

Check Point Antivirus 軟體刀鋒能防止並阻擋如惡意軟體、病毒和木馬程式等威脅進入和感染網路，使用多個惡意軟體偵測引擎來保護您的網路，包含特徵和行為式引擎。當惡意軟體試圖進入或離開您的網路時就會被發現。

防止存取惡意網站

Antivirus 軟體刀鋒會掃描傳出的 URL 要求，並能確保使用者不會瀏覽已知會散布惡意軟體的網站。ThreatCloud 中超過 30 萬個網站的資訊會即時更新到閘道。

發現和阻擋未知的惡意軟體

Antivirus 軟體刀鋒經過設定後，可以偵測出可能有惡意的可疑執行檔。它會在一個受保護的沙盒環境中啟動這些可疑檔案，監控這些檔案是否會試圖改變作業系統或登錄檔來判斷出其是否為惡意。如果檔案被判定為惡意，則會阻止它進入網路。

統一式的惡意軟體和殭屍程式防護

Antivirus 軟體刀鋒可以和 Anti-Bot 軟體刀鋒整合，讓組織有能力進行早期和後期防護，並可以提供多層式的威脅防禦能力。系統管理員可以在單一個使用者介面中管理整合式的政策和報告。

Anti-Bot軟體刀鋒

Check Point Anti-Bot 軟體刀鋒可偵測出被殭屍程式感染的電腦，並且阻擋來自電腦犯罪份子指揮與控制 (C&C) 伺服器的通訊，防止殭屍程式造成損害。它使用一份由最大型的即時雲端安全威脅知識庫 ThreatCloud™ 持續更新的 C&C 位址清單，能在隱匿的殭屍程式造成損害和影響使用者前就先偵測出來。

殭屍程式的解決方案

Check Point 的威脅防禦解決方案包含 Anti-Bot 軟體刀鋒和來自 ThreatCloud™ 的支援，能提供時刻更新的安全情報給安全閘道，包含超過 2 億 5 千萬個位址的殭屍程式探索結果、超過 450 萬個惡意軟體特徵和超過 30 萬個遭到惡意軟體感染的網站。

THREATCLOUD™

ThreatCloud 是第一個對抗電腦犯罪的協同網絡。它能提供即時、動態的安全情報給安全閘道。這些情報可以用來識別新興的攻擊和威脅趨勢。ThreatCloud 能提供 Anti-Bot 軟體刀鋒所需的能力，可以在閘道檢查已知指揮與控制伺服器不斷改變的 IP、URL 和 DNS 位址。由於這個作業是在雲端進行，因此可以即時掃描數以百萬個特徵和惡意軟體防護。

ThreatCloud 的知識庫會彙整來自全球閘道的攻擊資訊而不斷更新，還會接收來自全球威脅感應器的饋入資訊，以及 Check Point 研究實驗室和業界最佳惡意軟體研究成果的情報。經過彙整的安全威脅資訊會分享給所有閘道使用。

功能優勢

找出已經存在電腦中的殭屍程式

阻擋 APT 攻擊

防止如竊取資料等損害

利用 ThreatCloud 的即時情報對抗不斷改變的動態威脅情勢

具備多種鑑識工具，可以容易地調查感染情形、評估損害和判斷後續步驟

利用整合式的威脅報告和儀表板觀看和管理「惡意軟體整體概況」

ThreatSpec™ 殭屍程式探索引擎

殭屍程式都是隱密的，經常會躲在電腦中，一般的防毒程式難以發現。Check Point Anti-Bot 軟體刀鋒能利用 ThreatSpect™ 引擎獨特的多層次探索技術，以及來自 ThreatCloud 最新的更新資訊，偵測出被殭屍程式感染的電腦。ThreatSpec 會彙整資訊以準確偵測出殭屍程式。

遠端操作者的位址，包含 IP、DNS 和 URL

偵測出獨特的殭屍程式通訊模式

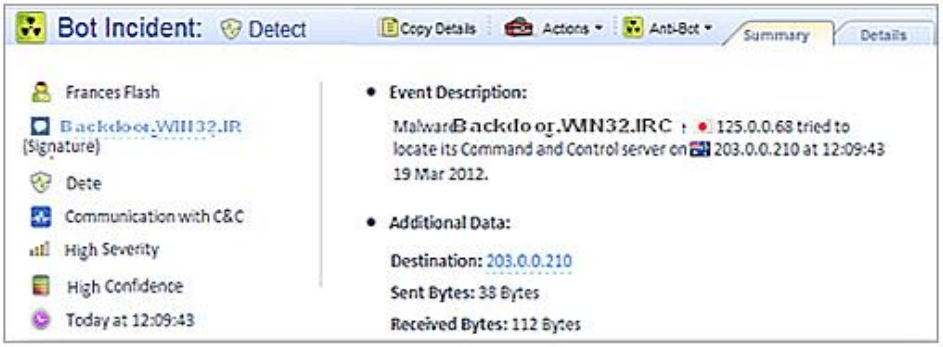
偵測如垃圾郵件或點擊詐欺等攻擊行為

阻擋殭屍程式的通訊

當偵測到殭屍程式後，Check Point Anti-Bot 軟體刀鋒會阻擋受感染電腦和 C&C 伺服器之間的遠端指令通訊，讓電腦犯罪者無法操作殭屍程式，並且避免組織遭受可能的殭屍程式損害。

調查殭屍程式的感染情形

利用先進的日誌和管理系統調查殭屍程式的感染情形，提供如受感染電腦/使用者、殭屍程式名稱、殭屍程式動作 (例如和指揮與控制伺服器通訊並傳送垃圾郵件)、傳送和接收的資料量，以及感染的嚴重性等。 此外，這個解決方案中還包括一個全方位的 ThreatWiKi，能讓安全團隊容易地瞭解他們所面對的殭屍程式 — 包括其徵狀、運作方式，以及任何可用的技術資訊。



統一式的惡意軟體和殭屍程式防護

Anti-Bot 軟體刀鋒可以和 Antivirus 軟體刀鋒整合，讓組織有能力進行早期和後期防護，並可以提供多層式的威脅防禦能力。系統管理員可以在單一個使用者介面中管理整合式的政策和報告。

整合到 Check Point 軟體刀鋒架構

Anti-Bot 軟體刀鋒可以完全整合到軟體刀鋒架構，讓客戶可以依變動的需求快速擴充安全防護，節省時間並降低成本。其可容易且快速地在現有的 Check Point 安全閘道上啟用，利用現有的安全基礎結構節省時間與成本。Anti-Bot 軟體刀鋒可以集中管理，讓組織可以從單一個使用者易於操作的主控台集中管理、實施政策，並且進行記錄。

URL Filter 網頁過濾軟體刀鋒

網頁過濾軟體刀鋒能協助您提供使用者安全的網頁瀏覽環境，全動態的雲端資料庫，提供了超過 2 億多筆的網頁資料，並可透過 UserCheck 的功能，加強使用者上網安全資安意識。

功能優勢

強大且動態的網頁過濾技術，超過 2 億多筆的網頁資料庫與預先定義好的 64 種網頁分類，方便管理者利用分類來進行政策設定。

可針對 SSL 封包進行過濾或者選擇精簡的 SSL 網頁過濾，來降低管理複雜度。

與應用程式管理 APCL 軟體刀鋒整合，提供最佳的 web 2.0 資安防護效能。

SandBlast雲端沙箱軟體刀鋒

Check Point SandBlast 刀鋒是一個可以防範新型入侵程式、尚未發現威脅和目標式攻擊感染系統的解決方案。傳統的解決方案專注在偵測，只能在威脅攻入網路之後發出通知。Check Point 最新的沙箱技術可以將新威脅阻擋在外，不讓感染的情形發生。由於沒有感染發生，因此也不需要感染修補作業的時間、人力和負擔。

在過濾掉合法檔案之後，可疑檔案會雲端進行模擬。我們會分析模擬檔案的行為，判斷其是否具備惡意軟體的特性，包含異常系統登錄檔變更、建立新檔案、網路連線或竄改系統等。新識別出來的惡意軟體會立刻被阻擋，然後建立對應的攻擊特徵並立即發佈到 ThreatCloud。Check Point SandBlast 是 Check Point 多層式威脅防禦解決方案的關鍵性新增元件，增加了對未知威脅的防護。

主要優點

在防毒特徵碼製作完成前防範未知的惡意軟體

阻擋針對多重 Windows 作業系統環境發動的攻擊

最廣泛的檔案測試防護，以分析和偵測惡意軟體

可利用雲端達到容易且彈性的部署

零誤報能力讓您保護網路時可以無須阻擋業務流程

集中式管理可以節省時間和降低營運負擔

CPU-Level 偵測沙箱，提高準確率並且避免惡意軟體規避掃描

Check Point SandBlast 軟體刀鋒特色

虛擬沙盒功能

Check Point SandBlast 刀鋒會攔截和過濾下載檔案，在虛擬環境中執行它們，然後標記出會觸發可疑或惡意行為的檔案。常見的惡意軟體行為包括修改登錄檔、網路連線、建立新檔案、修改 DNS 等。當發現新威脅時，檔案的特徵會送到 Check Point ThreatCloud，讓這個新惡意軟體成為已知且有記錄，以便所有 Check Point 的實體和虛擬設備可以加以阻擋。

ThreatCloud

Check Point SandBlast 和 Check Point ThreatCloud 一起運作，當全球 SandBlast 系統發現新惡意軟體時，就能接收到最新和零時差威脅的更新。每一個新發現的威脅特徵都會派送到其他正在連線的 Check Point 閘道，在威脅擴散前加以阻擋。這個持續的協同作業讓 SandBlast–ThreatCloud 這組生態系統成為當今最先進和最新的威脅網路。

支援多個模擬作業系統

Check Point Threat Emulation 可以同時提供多個 Windows 作業系統的模擬環境。

MS Office 和 Adobe 檔案

Check Point Threat Emulation 能補強我們已經是領先業界的 MS Office 和 Adobe 檔案保護。MS Office 和 Adobe 檔案是最容易被忽略和遭受攻擊的管道，同時還是最常傳遞的檔案。

加密式攻擊

利用 SSL 和 TLS 傳送檔案，代表這是一個可以躲避許多產業標準實作的安全攻擊管道。Check Point SandBlast 刀鋒能阻擋內部 SSL 和 TLS 通道，以便取得和啟用檔案，找出這些受保護的串留中是否躲藏著威脅。

可與軟體刀鋒架構整合

Check Point SandBlast 可以當成個別服務購買，或是連同預先選購的 Check Point 軟體刀鋒一起購買。Check Point 軟體刀鋒架構是第一個也是唯一一個可提供完整、彈性和可管理的威脅防禦給所有企業的架構。軟體刀鋒具備無與倫比的彈性和擴充性，能以較低總持有成本提供具效益的防護，以符合企業今日或未來的需求。

彈性化部署

Check Point SandBlast 可以和現有的網路一起實作，利用 Check Point 的 ThreatCloud 進行模擬。可以在任何閘道上，利用 Check Point 管理主控台管理模擬和報告作業。