

Symantec[®] WebPulse

掌握全球最新網站脈動，WebPulse 協同防禦技術概觀：
於 Symantec 全球情資網路中的核心角色



目錄

簡介

Symantec 網頁安全架構

Symantec 情資服務／WebPulse：整體架構概觀

建議採用的惡意軟體防護功能

WebPulse 技術概觀

單一 URL 可套用多重類別

結論

簡介

網頁已成為幾乎所有企業不可或缺的一部分。與此同時，社群媒體也讓網頁環境變得動態且複雜——為惡意軟體以日益隱密且精密的手法擴散，提供了絕佳溫床。

這種不斷演變的環境，使得網頁存取與頻寬使用的管理更加困難，同時也帶來了唯有網頁代理伺服器(web proxy)才能妥善因應的資安挑戰。網頁資安解決方案必須具備準確的網站分類與風險評估能力、全球涵蓋範圍，以及針對從未見過之 URL 的即時分類能力，這些都至關重要。

Symantec[®] WebPulse 是 Symantec 全球情資網路(Global Intelligence Network，簡稱GIN)的一環，是一套專為善用使用者行為驅動之力量而設計的雲端基礎架構，能將使用者輸入的資料轉化為全球網頁情資與網頁威脅情資。我們相信，WebPulse 自 2004 年推出以來，始終是業界最先進、最具實用性的網頁資安技術。

Symantec GIN 是一套協同防禦雲端服務，整合來自逾 15,000 家不同企業、1.75 億名 Symantec 端點防護使用者，以及 Symantec 電子郵件資安產品所掃描之數十億封電子郵件的資料輸入，藉此為 Symantec 安全網頁閘道解決方案提供強大後盾。

WebPulse 運用多種技術分析上述輸入資料，提供業界最快速、最準確的網頁分類與評等。在 WebPulse 架構中，每一筆傳入的 URL 請求，都會經過多種自動化與人工威脅分析方法的層層處理。

WebPulse 運用其雲端基礎架構，將網頁情資提供給 Symantec Edge 與 Cloud Secure Web Gateway。WebPulse 能無縫遞送頻繁的資料庫更新，以及新型防禦措施(例如：新的分析方法與新增語言支援)。使用者無須更新其設備或 SaaS 服務，即可立即受惠於這些新防禦措施與更新。

Symantec 威脅研究團隊——分布於全球九個研發中心、逾 3,500 名研究人員——為 WebPulse 與全球情資網路提供強力支援。

本文件旨在深入說明 WebPulse 協同防禦機制，此機制是 Symantec 預測式資安防禦不可或缺的一環。

Symantec 網頁安全架構

先發制人且分層式網頁防禦：僅偵測並封鎖已知威脅的做法，已不再有效。隨著惡意軟體手法日趨精密，加上「低投入、高滲透」的量產型惡意軟體崛起，網頁資安解決方案必須能夠預先掌握惡意軟體動向，才能在企業遭受感染之前將其攔截。

一套預測式、分層式的網頁防禦，需要具備以下五大關鍵要素：

- 全球協同雲端情資基礎架構——須具備以下條件：
 - 一套整合式、群眾外包(crowd-sourced)的生態系統，能運用每日合計瀏覽數千萬個網頁之真實使用者的經驗。
 - 一套雲端基礎架構，能運用多種威脅偵測引擎、機器分析及人工評等人員，彙整並分析來自社群的資料。
- 即時內容過濾：
 - 在全球協同情資系統的支援下，即時內容過濾結合了動態防護與精細的類別控管能力，滿足企業落實可接受網際網路使用原則所需的需求。
 - 廣泛的類別涵蓋範圍，加上可為單一URL指定多重類別的能力，提供管理當今複雜網頁環境所需的多維度控管。
- 內嵌式威脅偵測：現今的內嵌式威脅分析本身已是多層式架構，同時也是預防式網頁資安解決方案不可或缺的一環。由於愈來愈多惡意軟體潛藏於SSL加密流量中並將其作為通訊管道，因此必須對SSL加密流量進行檢查。此外，也必須檢查經使用者驗證後自網頁下載的軟體、透過網頁郵件(webmail)傳送的附件及其他內容。此環節不應僅止於基本的防惡意軟體掃描，還應涵蓋封鎖清單／允許清單(block listing/allow listing)、行為分析(含靜態程式碼分析)、沙箱(sandboxing)、機器學習等技術。
- 網頁與雲端應用程式及內容控管：此層級涵蓋網頁內容、雲端及網頁應用程式控管機制，可防止來自未知網站的下載行為、偵測偽裝檔案，並依使用者、群組或其他原則變數，允許或拒絕特定網頁應用程式或其操作(例如：張貼訊息或上傳附件)。
- 遠端與行動使用者防護：遠端與行動使用者的人數持續攀升，而他們所需的防護層級，應與企業辦公室內的使用者相同。透過網頁過濾用戶端或 SaaS 服務延伸 WebPulse 的防護範圍，可為這類使用者提供預測式防禦，並降低其將惡意軟體帶入企業內部網路的風險。

**內嵌式威脅分析是預防式
網頁資安解決方案中，不
可或缺的多層式關鍵要素**

附註

瞭解情資服務(Intelligence Services)背後的運作原理，是相當重要的一環。

許多以網頁為媒介的攻擊，一開始都是將指令碼植入受信任的網頁中。這些指令碼通常會透過動態且強大的惡意軟體遞送網路(MDN)，產生指向惡意軟體主機的動態連結。Symantec 情資服務的首要目標，是分析並封鎖指向惡意軟體本身的連結。使用者不應因此被阻擋而無法瀏覽受信任的網頁——指令碼本身並不會對端點造成危害。

這與網頁資安業界許多廠商所採取的做法有根本性的不同，也因此衍生出以下幾個問題：

- 這些廠商是否知道實際的惡意軟體位於何處？
- 若知道，為何還要封鎖僅是承載該連結、本身無害的網頁？
- 若不知道，既然已經找到該連結，為何仍無法得知惡意軟體的所在位置？

Symantec 情資服務／WebPulse：整體架構概觀

Symantec情資服務結合WebPulse協同防禦，在此多層式防禦架構中扮演多項關鍵角色，包括：預先因應零時差(zero-day)攻擊、阻止間諜軟體、甚至是遭殭屍網路(botnet)感染的系統向外「回報連線」(phone home)的行為，以及偵測網路釣魚與惡意廣告(malvertising)威脅。透過防止惡意軟體從網際網路下載，並搭配內嵌式進階威脅防護，此防禦機制得以發揮最大成效。

Symantec情資服務與WebPulse的設計定位，是作為進階威脅防護前線的高反應速度預防式防禦機制，而非用以取代進階威脅防護本身。WebPulse可簡單理解為一套基本的輸入輸出系統：龐大的輸入資料，來自逾15,000家企業客戶，包括使用Symantec Cloud與Edge代理伺服器、Security Analytics、Symantec Endpoint、電子郵件閘道(Email Gateway)的客戶，以及一般消費者使用者。

WebPulse就如同一個「黑盒子」，能進行即時分析並輸出URL分類結果與風險等級(Risk Level)評等，其輸出時間以毫秒計算，使用者可即時獲得回饋。WebPulse無須更新週期或修補程式，隨時保持在最新狀態。

WebPulse 運作方式

對URL的請求，會先比對代理伺服器上的本機情資服務資料庫，或其他Symantec產品上的本機分類快取。若該URL可在本機完成分類，即可運用該分類資訊來允許或封鎖此請求。

圖 1：WebPulse 處理流程



一般而言，本機無法分類的內容約占5%。若該URL未列於本機資料庫或分類快取中，系統會動態將該URL傳送至WebPulse。在雲端，該URL會先比對中央主資料庫，其運作方式與本機查詢類似：若該URL已列於主資料庫中，系統會將該URL的分類結果回傳給提出請求的WebPulse用戶端，供其用於允許或封鎖該請求，而此新結果也會自動快取於本機。

若該URL同樣未列於雲端的中央主資料庫中，系統將視情況運用動態即時評等(Dynamic Real-Time Rating，簡稱 DRTR)進行即時分析與分類。所得出的URL分類結果，將回傳給提出請求的WebPulse用戶端，供其用於允許或封鎖該請求。

WebPulse運用多種方法 (包括漏洞攻擊偵測技術) 分析指令碼，並偵測惡意 酬載與其所參照的網域

無論即時分類結果為何，URL都會同步傳送至多項背景處理程序。部分背景處理程序著重於為資料庫提供新的內容分類，另一部分則著重於搜尋惡意軟體活動的跡證。DRTR主要用於內容分類，但同時也用來記錄其所分析之每個URL的大量中繼資料(metadata)，而這些中繼資料正是驅動許多WebPulse背景處理程序的關鍵養分。許多URL並非網頁，因此不適合以DRTR進行分類，但WebPulse仍會盡可能蒐集該URL的相關資訊，以提供給背景處理程序使用。

WebPulse運用多種方法(包括漏洞攻擊偵測技術)分析指令碼，並偵測惡意酬載與其所參照的網域。當使用者透過WebPulse從未見過的URL存取二進位檔案時，WebPulse也會下載該檔案，並讓其通過最多十種不同防毒(AV)掃描引擎(具備完整啟發式偵測能力)、指令碼分析器(例如：具有heap spray手法的惡意Java指令碼)、漏洞攻擊偵測模組，以及其他惡意軟體偵測機制的重重檢驗。新型威脅可在數分鐘內完成識別，並自動新增至主要URL資料庫中，藉此保護其他客戶。這正是WebPulse雲端使用者受惠於彼此協作所產生之網路效應的方式之一：即使僅有極少數防毒廠商能夠偵測到新型網頁威脅，WebPulse使用者仍能獲得廣泛的即時防護，並對這些威脅做出強而有力的零時差回應。

除了Symantec自身的分析之外，系統也會評估納入多個涵蓋惡意軟體與網路釣魚網站的第三方 URL 資訊來源，供主資料庫收錄。此外，當搭配 Symantec Content Analysis 使用時，Edge Gateway可將Content Analysis判定為惡意軟體來源的任何URL，傳送至WebPulse服務進行驗證。值得注意的是，惡意軟體資訊來源在納入情資服務資料庫之前，都會先經過品質檢核，以避免誤判(false positive)。

針對與資安相關的類別，系統會每五分鐘將漸進式資料庫更新推送至代理伺服器，讓本機防禦機制能盡可能以本機資料庫回應請求，藉此維持效能表現。若發現任何URL無法在本機資料庫中找到相符項目，代理伺服器便會向WebPulse查詢。

建議採用的惡意軟體防護功能

Symantec Secure Web Gateway解決方案具備廣泛的功能組合。以下段落將簡要概述幾項實用且建議採用的惡意軟體防護功能。

URL 過濾

這是攔截對已知惡意軟體來源之請求的第一道防線。對於未知或未列於本機資料庫中的URL，Cloud或Edge SWG會連線至WebPulse協同防禦服務，針對未分類的URL進行即時分析。

驗證

驗證使用者身分最安全的方式，是針對每個新工作階段(session)進行驗證。若某台桌上型電腦遭惡意軟體感染但尚未通過驗證，便無法與網際網路上的系統進行通訊，藉此阻斷任何機密與個人資料可能外洩的風險。

資料類型控管

若使用者本就無權在其桌上型電腦安裝軟體，那麼他們為何還能從網際網路下載執行檔？封鎖執行檔是防範惡意軟體的另一項重要措施。惡意軟體經常會試圖下載軟體，藉此在受感染的桌上型電腦中植入惡意內容。

檔案類型的封鎖，可依據真實檔案類型偵測結果來執行。

最佳實務建議，對一般網際網路使用者全面封鎖執行檔。

封鎖執行檔的另一項理由，在於惡意動態連結可能會指向會被安裝至桌上型電腦中的惡意執行檔，而封鎖執行檔即可防範此類威脅。

檔案類型的封鎖，可依據真實檔案類型偵測結果來執行。Symantec 最佳實務建議，對一般網際網路使用者全面封鎖執行檔；若此做法無法接受，至少也應針對未分類及／或威脅風險等級(Threat Risk Level)偏高的網站，封鎖執行檔下載。當僅依賴檔案類型與分類已無法滿足企業需求時，威脅風險等級是一項極為實用的工具，可用於微調並客製化網頁資安防護。如需進一步資訊，請參閱 Symantec Threat Risk Levels 白皮書。

通訊協定合規性

Symantec Edge 與 Cloud Secure Web Gateway 針對多種通訊協定採用應用程式代理伺服器機制。由於連線區分為用戶端與代理伺服器之間、以及代理伺服器與伺服器之間兩段，因此可過濾掉如緩衝區溢位攻擊(buffer overflow attack)等通訊協定層級的威脅。代理伺服器會將(由伺服器傳向代理伺服器的)通訊協定行為，轉換為(由代理伺服器傳向用戶端)符合 RFC 規範的行為。

SSL 攔截

SSL加密流量通道，需要透過安全網頁閘道解決方案來因應。在代理伺服器端終止(terminate)SSL連線，可偵測惡意內容與通道化(tunneled)應用程式。憑證管理機制可用於驗證 X.509 憑證，並僅允許受信任的用戶端或伺服器憑證通過。此外，代理伺服器也可封鎖企圖透過 443 連接埠傳出的非 SSL 流量——此類流量可能是惡意軟體感染的徵兆。

進階威脅防護與惡意軟體掃描

惡意軟體防護的最後一道步驟，是內嵌式惡意軟體掃描。透過延伸 Cloud 與 Edge SWG 的內容檢查能力，並以 Symantec Content Analysis 引擎為後盾，可對輸入與輸出資料進行惡意軟體掃描。根據預設設定，所有流量(包括大型檔案)皆會經過 Content Analysis 的掃描。

Content Analysis——內含於 Symantec Web Protection Suite 及 Symantec Network Protection之中——透過多層檢查機制提供進階威脅防護，包括：以雙重防惡意軟體引擎進行惡意軟體特徵碼掃描、靜態程式碼與行為分析、封鎖清單／允許清單、機器學習，以及提供內建(on-box)沙箱或雲端沙箱、抑或串接外部沙箱解決方案的能力。相較於多數其他採用傳統威脅防護及／或選擇性掃描做法的安全網頁閘道解決方案，此進階威脅防護能力是一項極具價值的差異化優勢。

日誌檔分析／報表

建議定期檢查存取日誌檔，且檢查頻率應足以掌握正常流量的樣態，以便及時發現並調查新出現、異常或不尋常的流量。Symantec Reporter 是分析存取日誌檔的絕佳工具。

附註

通常由Edge代理伺服器傳送至WebPulse的內容，多半是本機資料庫無法分類的內容。不過，若有必要，已分類為「網頁代管」(web hosting)的URL，也同樣會傳送至WebPulse進行即時分析，以套用更準確的分類結果。

WebPulse 技術概覽

分類準確度

準確度是指過濾產品能以最低的誤判(false positive)率，正確分類URL的能力。換言之，準確度所回答的問題是：在該過濾產品歸類為X(例如色情、間諜軟體或賭博)的100個URL當中，實際確實屬於X類別的比例為何？

比例愈高，代表過濾產品的準確度愈高。漏判(false negative)則是另一項準確度指標，此時所要回答的問題是：有多少屬於X類別的項目遭到遺漏？Symantec技術所提供的分類準確度，在所有網頁資安廠商中居於領先地位。WebPulse能依據多個層級對URL進行分類：

- 網域(Domain)：symantec.com底下的所有主機，可套用相同類別
- 主機(Host)：host1.symantec.com與host2.symantec.com可套用不同類別
- 目錄(Directory)：host1.symantec.com/directory1與host1.symantec.com/directory2可套用不同類別
- 檔案名稱(File name)：host1.symantec.com/directory1/good_file.jpg與host1.symantec.com/directory1/malicious_file.jpg 可套用不同類別
- 查詢字串(Query string)：www.facebook.com/?sk=inbox與www.facebook.com/?sk=ff 可套用不同類別
- IP位址：基於效能考量(避免反向DNS查詢)，可將以IP位址為基礎的分類新增至資料庫中
- 通訊協定與標頭(header)分析，是另一項可運用的分類選項

單一 URL 可套用多重類別

網頁內容並非總能輕易歸入單一類別。舉例來說，www.facebook.com/?sk=inbox 這個網址，同時兼具社群網路網站與 Facebook 內建電子郵件應用程式這兩種性質。準確的網頁過濾機制能辨識此一情況，並將該網站同時歸入這兩個類別，讓企業能夠靈活控管使用者可存取該網站的哪些部分。情資服務最多可為單一網頁提供四個類別，能更準確地反映網頁內容，並可組合出數千種精細的子類別，實現靈活且強大的原則執行能力。

防止使用者規避內容過濾原則

為達到高準確度，WebPulse 能透過準確分析並分類以下工具類型，防止使用者規避內容過濾原則：

- 提供線上語言翻譯服務的翻譯網站
- 快取過往內容、供使用者選擇瀏覽的封存網站
- 由搜尋引擎提供的圖片搜尋結果
- 透過通常不易察覺的中介網站來轉發請求的代理匿名服務(proxy anonymizer)

早期世代的過濾技術，通常僅能提供表面性的分類結果(例如翻譯網站、圖片搜尋或封存網站)，但這對落實原則並無實質助益。客戶並不希望封鎖所有圖片搜尋，或所有翻譯與封存請求。相對地，Symantec 解決方案能夠辨識出嵌入於中介頁面中的目的網頁，藉此做出準確且實用的分類。舉例來說，情資服務能將 cnn.com 的封存頁面準確分類為新聞類別。

Symantec解決方案能夠 辨識出嵌入於中介頁面中 的目的網頁，藉此做出準 確且實用的分類

品質檢核

WebPulse 基礎架構配有一套嚴謹的品質檢核機制，旨在降低誤判與過度封鎖的情形。所有分類變更與惡意軟體辨識結果，都必須先通過 Symantec 專有的品質檢核，才會發布給客戶群使用。

效能

談到 WebPulse，效能是不可忽略的重要面向。情資服務與 WebPulse 提供高度可擴充、高效能的解決方案，僅有一小部分的整體網頁流量，需要由 WebPulse 進行即時分析。

網頁過濾功能經過最佳化，可於代理伺服器端(on-proxy/on-box)執行。分類請求會於記憶體(RAM)中處理，速度通常比在裝置外(off-box)執行快上一個數量級。企業或教育機構使用者所請求的網頁，情資服務通常能在代理伺服器端於8毫秒(ms)內完成約95%的分類；至於其餘5%，系統可即時、無感地向 WebPulse 主資料庫(通常於70毫秒內)或 WebPulse 動態即時評等(Dynamic Real-Time Rating，通常約需200毫秒，惟實際所需時間會因該網站的效能表現而有所差異)提出分類請求。在代理伺服器端處理分類請求，是能兼顧高效能與高可擴充性的最快架構——這也是為何 Symantec 針對資安相關類別每五分鐘提供一次漸進式資料庫更新，至於非資安相關類別，則每六小時更新一次。

裝置端(on-box)資料庫同時也收錄了最常見網站的 IP 位址，避免 DNS 反向查詢拖慢 URL 的處理速度。

動態即時評等與動態連結分析

WebPulse提供超過300個資料庫(library)，可即時為新內容進行評等與分類。即時分類功能支援超過六十種語言，並包含Pornovian——一款用於偵測色情相關內容的通用模組。此功能與其他多項威脅偵測功能，皆為 WebPulse 的關鍵組成要素，兩者相輔相成，成為 WebPulse 的另一項獨特差異化優勢。

即時威脅偵測涵蓋動態連結分析(dynamic link analysis)功能：當網路犯罪者於受信任的網頁上植入指令碼，強迫瀏覽器從通常尚未分類且快速變換的惡意軟體主機下載惡意內容時，即會運用此項功能，並將涉嫌違規的 URL 即時傳送至 WebPulse。

即時分類功能會拆解網頁並分析其組成元件，以下列舉部分用於指派類別的資訊類型：

- 語言(範例：英文)
- 原始碼語言(例如：JavaScript)
- 文件類型(範例：HTML)
- 字元集(範例：UTF-8)
- 外部連結類別
- 內容文字
- 指令碼
- Iframes

即時惡意軟體偵測模組

多數即時惡意軟體偵測模組，會針對內容（資料或流量）中可能顯示危險徵兆的特徵進行檢查；同時，這些模組也會運用超過十三年來持續掌握網際網路灰色地帶動態的經驗，評估來源是否存在危險跡象。當特徵組合足夠可疑時，即會觸發示警。這些模組會探究：不良內容與合法內容有何不同？這些內容是以何種方式提供？又是從何處提供？一旦觸發即時惡意軟體偵測模組的回應，對可疑內容的存取即可立即遭到封鎖。

URL 背景檢查器

背景檢查器系統包含兩個模組：一個前景(即時)模組，以及一個用於檢查URL或網站背景資訊的背景(離線研究)模組。研究模組會蒐集有關惡意軟體遞送網路(Malware Delivery Network，簡稱MDN)的資料，讓即時模組得以判斷：此URL是否隸屬於這些網路之一？指向MDN的URL存取請求，可立即遭到封鎖。

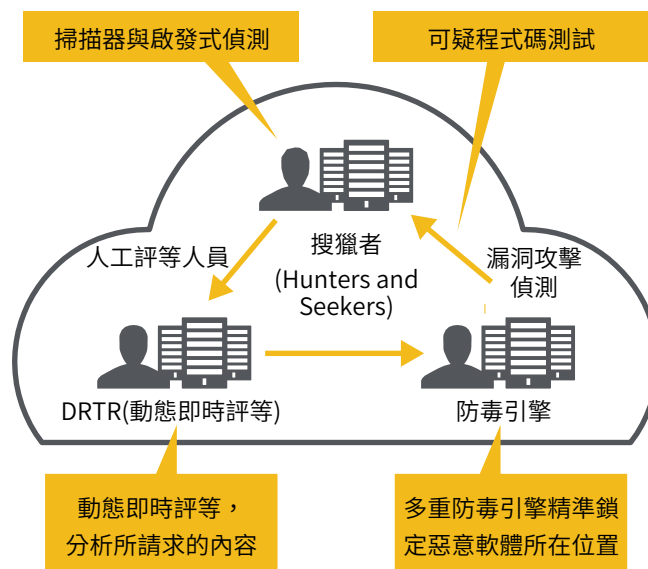
背景分析技術

並非所有分析都能即時完成。當資訊不足以做出即時判斷，或內容本身不適用於即時分類時，即代表已跨越即時分類與背景分類之間的界線。對於無法即時分類的少量內容(通常低於2%)，背景分析服務會運用精密的專有技術進行處理，並將分析結果回饋至WebPulse主分類資料庫。最後一道步驟，則是由人工評等人員持續訓練DRTR與各項背景系統，並針對罕見網站進行調查與分類。

背景系統同時也會處理已完成即時分類的URL，以判斷該分類結果是否應納入資料庫——這也代表並非所有經過即時分類的URL，都會被加入資料庫中。決定是否將某URL納入資料庫的判斷準則之一，即為其單位時間內的請求次數。

背景系統會持續尋找額外的佐證資料，以補充即時蒐集到的資訊。一旦識別出這些資訊，即可用於微調並更新即時分類模組。以HTTP參照來源標頭(referrer header)為例：只要掌握參照來源的相關資訊，WebPulse便能分析網頁攻擊的完整路徑。在許多情況下，惡意軟體主機僅會在請求中包含特定參照來源(例如：搜尋引擎結果)時，才會顯示其惡意內容。

圖 2：背景分析技術



並非所有分析都能即時完成。當資訊不足以做出即時判斷，或內容本身不適用於即時分類時，即代表已跨越即時分類與背景分類之間的界線

持續評估使用者所存取之 所有網站的相關風險，是 相當重要的一環

Symantec獨有的偵測機 制，往往能在網站出現於 任何第三方網路釣魚清單 之前，便率先將其偵測出 來

惡意軟體偵測

面對瞬息萬變的威脅態勢，有效的惡意軟體防護，需要一套廣泛的偵測機制作為後盾。WebPulse 技術結合以下分析與識別技術，發展出一套獨特的網際網路流量惡意軟體防護做法。

惡意流量偵測與分析

為識別惡意軟體散布機制(包括中介站點與惡意軟體主機)，WebPulse內建多套規則引擎，能靈活因應瞬息萬變之威脅態勢下的各種流量與網站類型。這些規則會依據 Symantec 惡意軟體專家所識別出的即時資訊，持續進行微調、擴充與更新，讓您無須耗費心力，親自鑽研成為網頁防禦專家。

惡意網站與內容識別及分析

持續評估使用者所存取之所有網站的相關風險，是相當重要的一環。即使惡意軟體已遭刻意混淆(obfuscated)，只要其嵌入於信譽良好的網站中，仍可被識別出來。Symantec透過多種方式進行此項分析：

惡意網站指紋辨識

為跟上惡意網站變換網域的速度，WebPulse 運用先進的指紋辨識模組，能快速識別出現在新伺服器上的類似網站。

網頁信譽評等

WebPulse 會蒐集網站的多種信譽相關資訊，自動為網站的信譽評分，並將資安風險偏高的網站歸類為可疑網站。

惡意 JavaScript 偵測

WebPulse 會記錄每日數百萬個網頁請求中所涉及的 JavaScript 相關資訊。Symantec 研究人員運用這些情資，識別出顯示可疑行為的特徵，並針對這些特徵研擬相應的新防禦措施。

惡意軟體內容分析器

WebPulse 具備專有的分析器，能運用統計分析技術，即時識別惡意網站，並在網頁中定位可疑內容。

網路釣魚偵測

WebPulse 內建專有的即時演算法，能識別偽裝成金融機構的網路釣魚網站。這些演算法搭配 WebPulse 對客戶所提出之未分類網站請求的即時處理能力，幾乎能即時發現新型網路釣魚威脅。Symantec 獨有的偵測機制，往往能在網站出現於任何第三方網路釣魚清單之前，便率先將其偵測出來。

與 Content Analysis 及 Malware Analysis 的整合

Symantec 進階威脅偵測引擎——Content Analysis 與 Malware Analysis——運用機器學習、行為分析、封鎖清單／允許清單、雙重防惡意軟體掃描及沙箱等技術，為 Cloud 與 Edge Secure Web Gateway 解決方案再添一層防護。除了提供此額外防護層之外，這兩項引擎也會將新型威脅的偵測結果，直接整合並分享至 Symantec 全球情資網路，讓新發現的風險能立即分類並納入 WebPulse 資料庫。

非法或可疑網站（詐騙網站）偵測

背景檢查器（及部分其他模組）可用於鎖定任何規模龐大且結構複雜的網站網路，而許多詐騙網路恰好符合此一特徵。部分大型惡意軟體遞送網路，本身也包含經營此類內容的子網路；背景檢查器會即時封鎖此類內容（初始分類通常會標示為「可疑」）。

第三方情資

第三方情資用於輔助Symantec自身的研究與分析工作。除了上述各項技術之外，WebPulse也會蒐集來自眾多第三方情資來源的資訊，包括商業惡意軟體與網路釣魚清單、社群貢獻的內容，以及對整體網頁資安威脅態勢所進行的一般性研究與持續監控。第三方來源的資訊，必須符合極高的品質標準，並通過一系列嚴格檢核，才會被納入WebPulse系統中。

活躍使用者社群

全球 WebPulse 社群，由來自逾 15,000 家不同企業客戶的使用者所組成，這些使用者在確保 WebPulse 服務的準確度與成效上，展現出高度的積極參與。他們每週向 WebPulse 傳送數十億筆新的網頁請求，讓此服務能清楚掌握大量新增與變動網頁區域的最新現況——而在這些龐大數量之中，也隱藏著最可能的網頁威脅來源位置，以及通往這些威脅的隱密路徑。Symantec 致力於對社群提出的請求與意見回饋進行調查與回應，通常可於 24 小時內完成。

WebPulse 社群，讓 Symantec 得以逐秒取得流經網際網路之所有流量的重要樣本。WebPulse 運用前述的惡意內容偵測技術，分析流量、網站與內容，達成極高的惡意軟體識別率。WebPulse 社群的使用型態及其即時分析能力，為使用者提供了無可取代的深入洞察，並為 Symantec 客戶提供盡可能最高等級的網頁威脅防護。

WebPulse 使用者可立即取得惡意內容識別結果

WebPulse 能確保您在需要防護的當下，立即取得所需資訊。只要某項分類、評等變更或惡意軟體識別結果通過 WebPulse 的品質檢核，所有 WebPulse 使用者便能立即取得該資訊。連線至 WebPulse 的用戶端，可即時向雲端服務查詢，藉此取得最新的分類或評等結果。

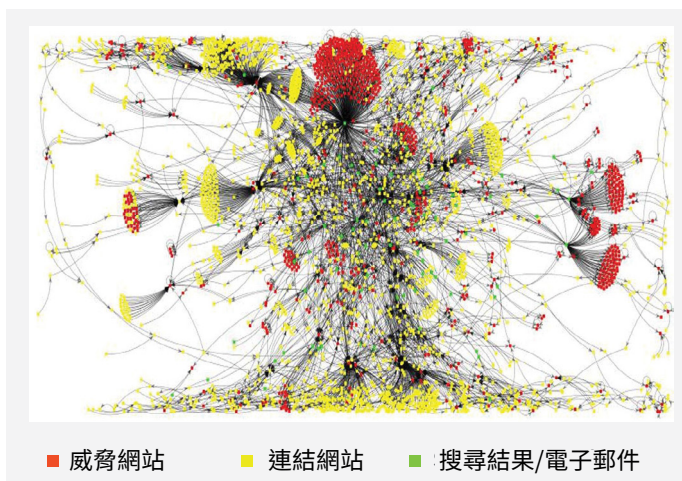
惡意軟體遞送網路分析

網路犯罪者會經營龐大的網站與伺服器網路，用以蒐羅受害者、將其導向指定地點、進行感染或誘騙、收取款項、提供新版或升級版的酬載，或進行其他操作。如同任何主流的網頁架構一樣，這些網路同樣具備備援、容錯移轉、備份與管理機制。然而，這類惡意軟體遞送網路也存在一項致命弱點：其規模與複雜度，恰恰為 WebPulse 提供了廣大的攻擊面 (attack surface)，可供其偵測與反制。

Symantec 技術長期累積的雲端經驗，加上其龐大的網頁流量，成為開發識別並追蹤 MDN 之系統的堅實基礎。WebPulse 每天都會自動識別出數千個隸屬於已知 MDN 的新網站與伺服器，無論這些 MDN 所提供的新漏洞攻擊與酬載偽裝或加密得多麼隱密，都能藉此保護我們的使用者免受其害。

WebPulse 能確保您在需要防護的當下，立即取得所需資訊

圖3：透過圖形化對應(mapping)軟體，可清楚看出圖中央的大型惡意軟體遞送網路，如何將毫無戒心的使用者捲入攻擊之中



網頁應用程式與應用程式操作控管

除了 URL 與 IP 位址之外，情資服務資料庫也收錄了與網頁應用程式相關的資訊：

- 應用程式名稱（範例：Facebook）
- 應用程式操作（範例：張貼訊息）
- 應用程式類別（範例：社交網路）

上述資訊可用於建置精細的原則，藉此控管網頁應用程式的使用。新的應用程式與應用程式操作，可直接套用並提供給Cloud與Edge SWG客戶使用，無須額外更新。由於此類資訊已納入資料庫，因此所有異動內容，皆可透過內容原則語言(Content Policy Language，簡稱 CPL)及視覺化原則管理員(Visual Policy Manager，簡稱 VPM)於 Edge Proxy 上取得；至於 Cloud Proxy，則會於自動化資料庫更新安裝完成後隨即套用。如有需要，亦可搭配 Symantec CASB 取得額外的應用程式可視性與控管能力，其可識別超過 35,000 種應用程式。

Symantec Edge 與 Cloud SWG 的報表功能，只要有新的應用程式或應用程式操作可供使用，便會立即顯示。

網頁應用程式與應用程式操作異動管理

網頁應用程式控管的關鍵環節之一，在於及早偵測應用程式的異動狀況，以便即時進行調整。系統已針對所有受支援的應用程式與應用程式操作，建立一套品保(Q&A)流程；系統會持續監控各應用程式與操作項目，一旦偵測到異動，便會立即採取行動，並透過標準資料庫更新機制推送相關變更。

系統已針對所有受支援的 應用程式與應用程式操作， 建立一套品保(Q&A) 流程

Symantec Security Labs 持續投注人力、設備與合作關係，藉此建立並強化我們的內部專業能力

結論

Broadcom 產品持續演進其網頁資安解決方案，以預防並對抗快速變化的網頁威脅。這些解決方案之所以能為客戶帶來強大優勢，關鍵在於充分運用以下要素：

- 雲端：WebPulse作為情資服務的雲端服務元件，已持續開發長達十三年之久——是所有雲端資安解決方案中歷史最悠久的一項。此優勢讓我們得以在不影響客戶的前提下，持續強化並升級其功能——客戶無須自行下載或管理修補程式。這也讓Broadcom產品在因應不斷變化的威脅時，展現出所有廠商中最出色的靈活應變能力。
- 社群：憑藉來自業界規模最大使用者群的輸入資料，WebPulse 得以充分掌握使用者當下於網際網路上所遭遇的各種情況，為我們的資安研究工作提供寶貴的方向與重點。我們從未需要仰賴網頁爬蟲(web crawler)來搜尋內容。
- 防惡意軟體偵測技術：透過一套可靈活調整的雲端防惡意軟體技術組合，我們得以新增近期在準確度上有所提升、或針對特定威脅具備獨特能力的新型進階威脅掃描引擎，同時也能停用誤判率逐漸攀升至無法接受程度的掃描引擎。我們會持續監控並調整各系統(以及整體技術組合)的設定，以確保最佳的效能與準確度。
- 資安產業合作關係：隨著新的研究機構不斷出現，加上既有機構日益專精於特定領域，我們必須隨之調整與這些機構的合作關係，以確保資訊能快速交流，並持續演進應對新興威脅的協作流程。
- 持續擴展計畫：Symantec Security Labs 持續投注人力、設備與合作關係，藉此建立並強化我們的內部專業能力。
- 資安專業能力：Symantec 產品深植於將機器學習技術與人工研究人員相結合、形成共同回饋迴圈(joint feedback loop)的深厚根基之中。這是唯一能夠可靠因應每日龐大網頁流量管理挑戰的解決方案。



關於賽門鐵克

賽門鐵克是資安業界的長青樹，品牌享譽至今超過四十年。賽門鐵克(Symantec)已於2019/11併入全球網路晶片巨擘—博通(Broadcom，美國股市代號AVGO)，全世界網路網路流量有99.9%經過博通的網路晶片(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進核心技術、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，近年來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。(美籍華人王嘉康創辦的企業軟體安全公司，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

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术型領導廠商，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安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，以及基於比原廠更熟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。