

DragonSoft Web Protect or 2.0 特色與優勢

功 能	敘 述	效 益
智慧型全自動 網站防火牆	採取智慧型入侵行為辨識技術，提供使用者簡易的操作介面，阻斷各種意圖攻擊行為以強化網頁伺服器的安全性。	負責「保護」與「過濾」網站伺服器。過濾已知與未知的弱點攻擊，在層出不窮的攻擊中，保護網頁伺服器 並將異常的執行過濾掉。
SQL指令 植入式攻擊 SQL Injection	針對所攻擊之目標非資料庫本身之漏洞來進行而是一種未做好輸入驗證的問題。	DWP 擁有人工智慧精確辨識功能，能自動辨識夾藏在正常網站查詢命令中的攻擊指令，過濾可能造成傷害的 SQL 指令請求，避免資料庫資料外洩的風險。
緩衝區溢位 過濾防護 Buffer Overflow	利用指令或程式送出一大串資料到系統的緩衝區之中，而超出該記憶體區所限制的大小。如此系統程式便會當掉，而入侵程式便具備此程式系統的權限。	DWP 透過全中文的操作介面，管理者可以很簡易的設定 IIS Web Server 緩衝區的字元長度，如果接收到的指令字元超過可允許的設定值，DWP 將迅速啟動保護功能，有效避免緩衝區溢位（Buffer Overflow）攻擊。
HTTP指令 過濾防護	某些 HTTP 指令是使用者極少使用到及對系統有傷害的，如：GET、POST、PUT、OPTIONS、TRACE、HEAD、DELETE、COPY、MOVE、MKCOL、PROPFIND、LOCK、UNLOCK、SEARCH、BCOPY、BDELETE、BMOVE、BPROPFIND、BPROPPATCH、POLL、SUBSCRIBE、TRACK、UNSUBSCRIBE、CONNECT。	DWP 能精確辨識並自行定義由遠端攻擊者所送出的 HTTP 指令，一旦判斷出對 IIS Web Server 的資料有任何損害的疑慮，DWP 馬上執行過濾保護功能，管理者再也不用擔心惡意的攻擊。
ShellCode 過濾防護	標準的英語系網站是不執行高位元（High-Bit）傳送，但由於一些中文字或是特殊編碼以高位元訊息對 IIS 送出請求，這些都可能潛藏著欺騙式攻擊。當網頁伺服器使用的是多種語言的環境，需要去注意與過濾高位元存在網頁伺服器中。	DWP 完整的防護功能可以徹底避免潛藏的攻擊危機，管理者能夠輕易完成過濾設定，將可能潛在著欺騙攻擊的高位元（High-Bit）訊息完全過濾阻擋。

功 能	敘 述	效 益
多重編碼 過濾防護 Encoding Attack	藉由不同的【編碼】方式傳送給網頁伺服器去欺騙網頁伺服器原有的政策。	採用 DragonSoft 獨家智慧辨識模組，能夠洞悉遠端攻擊者是否意圖藉由傳送【多重編碼】來影響，網頁伺服器的正常運作，DWP 可精確辨識、精密分析、並確實防護，為網頁伺服器再加一道安全防護。
關鍵字串 過濾防護	一些惡意使用者傳送有傷害性的字串執行，像是 C:\WINDWOS\system32\cmd.exe 等的請求，造成網頁伺服器損害。	管理者可以用最簡單的方式自行設定關鍵字串，當 DWP 偵測到所接收的請求中含有會造成傷害的程式或指令時，DWP 將自動啟動防護機制，讓遠端攻擊者無可趁之機。
目錄跨越 過濾防護	攻擊者可利用【目錄跨越】這項弱點，針對受影響的系統進行擷取並刪除資料。	DWP 精準的辨識防護功能，能夠輕易的識破目錄跨越攻擊模式，並於第一時間啟動安全機制，使管理者無須擔心遠端攻擊者會跨越網頁伺服器根目錄的存取限制而取得資料存取權限。
目錄保護功能	可將網頁存放目錄或者其他目錄禁止讀寫防護。	讓管理者閱讀無障礙、無負擔的中文操作介面，只要經過輕鬆的勾選設定，DWP 就可以將所要保護的目錄設定在保護項目裡，防止重要資料受損或外洩，讓資料安全防護做到滴水不漏。
自訂警告訊息	於攻擊者畫面顯示警示訊息	管理者可利用簡單易懂的操作介面，事先自行設定相關警示訊息，一旦 DWP 偵測出攻擊訊息時，除了在第一時間啟動多層防護，確實完成安全防護佈屬外，還能將警示訊息顯示在攻擊者的瀏覽器上，讓惡意的入侵者知難而退。
全自動人性化	依造環境需求設定所需功能及政策	管理者可依照網路環境需求，設定所需要之防護政策，一旦設定完成後只需定時監看記錄檔來作分析，不需再花其他時間進行維護。

