

# 網站伺服器應用層防火牆 安全管理軟體



## DragonSoft Web Protector

## DragonSoft Web Protector

### 基本功能

- 支援 Windows Internet Information Service(IIS)網頁伺服器4.0、5.0、5.1
- 圖形管理介面，支援Windows NT/2000/2003/XP等多種作業系統環境安裝執行
- 全中文顯示介面與中文說明
- 內建支援三組網域，彈性輸入功能
- 具備SQL Injection阻擋功能
- 具備緩衝區溢位(Buffer Overflow) 攻擊之阻擋功能
- 具備未授權目錄存取之阻擋功能
- 具備未授權之HTTP指令阻擋功能
- 具備阻擋包含特定字串之網頁請求功能
- 具備阻擋包含ShellCode之網頁請求功能
- 具備阻擋目錄跨越之網頁請求功能
- 具備阻擋惡意編碼之網頁請求功能
- 具備阻擋植入木馬/後門之網頁請求功能
- 支援虛擬主機(VirtualHost)保護功能

### 進階功能

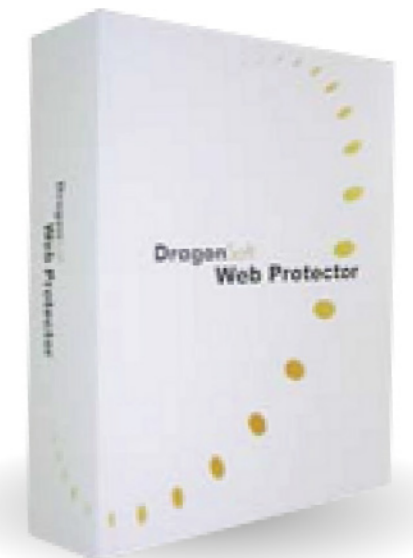
- 支援網站保護及攻擊來源之記錄(Log)功能
- 可自訂防護檔(Log)位置，可選擇儲存於他台主機，達到紀錄備援儲存目的
- 支援阻擋項目，過濾條件自訂增加與編輯功能
- 支援阻擋之警示頁面自訂，輕易轉換為各企業或機關資安管制頁面
- 網站防護及時顯示，防護時間/存檔位置顯示
- 可擴充支援至16組網域，提供網站伺服器全面防護要求

### 分析管理

- 支援多個網站之攻擊記錄集中由安全控制管理分析
- 支援多記錄檔(Log) 部分/全部、匯入合併資料，可分析更大時間區間下的網站安全變化
- 支援依照目標網站、日期範圍、攻擊來源IP、攻擊類型等..選擇分析
- 支援多樣化3D圖表統計分析顯示(長條圖、圓餅圖、曲線圖)
- 可依目標網站、日期範圍、攻擊來源IP、攻擊類型..等，分類產出3D圖表
- 可依目標網站、日期範圍、攻擊來源IP、攻擊類型..等，產出簡明(綜合/分類)記錄分析報表
- 可利用目標網站資訊，即時檢查被保護網站遭受攻擊情況
- 可利用日期範圍資訊，即時瞭解網站主機被攻擊時間頻率
- 可利用攻擊來源IP資訊，即時鎖定惡意人士IP加入其他安全阻擋方案進行阻絕
- 可利用攻擊類型資訊，即時檢視惡意人士攻擊語法內容，進階增加過濾字元

## DragonSoft Web Protector (For IIS) IIS網站應用層防火牆

DragonSoft Web Protector 採取過濾保護技術，分析探測 Web Server 往來中潛藏的不安因素，保護重要資料避免外洩，當DragonSoft Web Protector 探測挖掘出對 IIS Web Server 具有攻擊行為時進行過濾並偵測惡意行為的來源，將這些行為紀錄於系統，DragonSoft Web Protector 採取了日期、對方IP、類型匯入方式整合多種數據的一種【多元圖形化】方式呈現分析，協助IIS Web Server 安全狀況的控制與管理。



軟體安裝建議需求：Windows 2000、XP、2003 / IE 5.0以上、FireFox 4.0以上  
硬體建議需求：Pentium 3 Celeron 以上處理器/512MB以上記憶體 (無ECC) /40G 以上硬碟空間CD / DVD /高速乙太網路卡 / 無線網卡

亞太市場辦事處  
Tel: 886-2-8221-5408  
研發中心與營運總部  
Tel: 886-3-563-0989

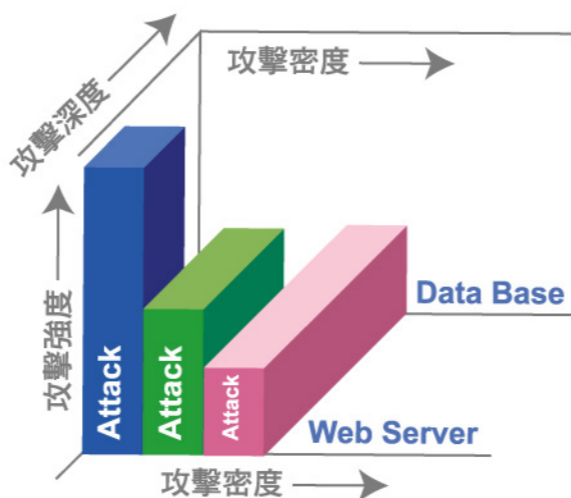
台北縣中和市中山路二段351號4樓之8  
Fax: 886-2-8221-5476 客服專線: 886-2-3234-999  
新竹市光復路一段 607 巷 30 號 6F  
Fax: 886-3-579-7758 e-mail: service@dragonsoft.com



## 企業最佳Web Server防護方案

據網路安全測試組織Sim Group表示有97%的網站門戶洞開，不堪一擊！

DragonSoft Web Protector企業網站安全最佳防護方案以人工智慧精準辨識各種惡意入侵行為，分析過濾資訊往來中潛藏的攻擊指令，透過簡易的全中文操作介面，輕鬆完成所有防護設定，確保所有重要資料不受任何損害，強化的安全性，搭配多元圖形化的安全分析報表，提供網站管理者最清楚、即時的系統安全資訊，徹底杜絕網站遭受惡意非法入侵及資料外洩的危機。



## DragonSoft Web Protector

DWP包含防護管制中心 (Protector Control Center) 與安全防護分析管理平台 (Protector Security Manager) 二大功能。不僅提供強大的阻擋防護與詳細紀錄被攻擊訊息紀錄，並提供後端多樣性分析，對於非法攻擊與惡意探索位址加入管控。

不僅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指令請求，避免資料庫資料外洩的風險。透過全中文的操作介面，管理者可以很簡易的設定緩衝區的字元長度，如果接收到的指令字元超過可允許的設定值，將迅速啟動保護功能，有效避免緩衝區溢位攻擊。能精確辨識並自行定義由遠端攻擊者所送出的指令，一旦判斷出對的資料有任何損害的疑慮，馬上執行過濾保護功能，管理者再也不用擔心惡意的攻擊。

## 關於DragonSoft

Dragonsoft為亞洲第一家獲邀加入國際安全評等機構CVE (Common Vulnerability and Exposure) 的資訊安全公司，並以優異的弱點偵防技術，成為該組織全球資訊安全協防的伙伴之一。

Dragonsoft專注並致力於網路安全軟體的研究與開發，以提供客戶更佳化的網路掃瞄服務與強化系統安全為目標，不僅建立完善的客戶服務機制，並是全球唯一提供完整中英文雙語安全弱點知識庫的資訊安全原廠。

## DWP入侵行為辨識技術

### SQL Injection

DragonSoft Web Protector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，避免資料庫資料的外洩的風險，確實保護IIS Web Server 的安全。

### Buffer Overflow 過濾防護

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，DragonSoft Web Protector 將過濾訊息並迅速啟動保護功能，有效避免緩衝區溢位(Buffer Overflow) 攻擊。

### HTTP 指令過濾防護

DragonSoft Web Protector 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危機，DragonSoft Web Protector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

DragonSoft Web Protector能徹底避免潛藏的攻擊危機，管理者能夠輕易地完成過濾防護設定，將可能潛在著欺騙攻擊的高位元(High-Bit)訊息完全過濾阻擋

### Encoding Attack 過濾防護

採用DragonSoft獨家智慧辨識模組，能洞悉遠端攻擊者是否意圖藉由傳送【多重編碼】來影響 IIS Web Server 的正常運作，DragonSoft Web Protector可精確辨識、精密分析並確實防護，為IIS Web Server 再加一道安全防護

### 關鍵字串過濾防護

管理者可以用最簡易的方式自行設定關鍵字串，當DragonSoft Web Protector偵測到所接收的請求中含有會造成傷害的程式或指令時，DragonSoft Web Protector將自動啟動防護機制，讓遠端攻擊者無可趁之機。

### Directory Traversal 過濾防護

DragonSoft Web Protector 精準的辨識防護功能，能夠輕易識破 Directory Traversal 攻擊模式，並於第一時間啟動安全防護機制，管理者無須擔心遠端攻擊者會跨越IIS Web Server 根目錄的存取限制而取得資料存取的權限。

### 目錄保護功能

讓管理者閱讀無障礙、無負擔的全中文操作介面，只要經過輕鬆的勾選設定，DragonSoft Web Protector就可以將所要保護的目錄設定在保護項目中，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

管理者可以利用簡單易懂的操作介面，事先自行設定的相關警示訊息，一旦DragonSoft Web Protector偵測出攻擊訊息時，除了在第一時間啟動多層防護，確實完成安全防護部署，還能將警示訊息即時顯示在攻擊者的瀏覽器上，讓惡意的入侵者知難而退。

