

# eB-Patrol™

## 網站內容即時防衛系統（標準版/專業版）

《臺銀採購部 LP5-970090 電腦軟體(政府版)/第四組/第58項》

### 防入侵篡改、即時回復、追蹤分析

根據 IDC 調查，72% 的企業有過網路駭客入侵的經驗。現今駭客猖獗，連防火牆及入侵偵測系統等有時亦抵擋不住駭客的入侵，導致網站的內容或檔案遭到駭客的篡改與刪除，且系統管理者往往無法即時修復已變更的內容，這不僅造成政府形象受損，在企業亦可能造成電子商務交易與商譽上的損失。網站內容被篡改已成為高度重視的問題，系統管理者必須採取主動式的安全機制，加強即時防護與復原功能，才能有效阻止層出不窮的網路威脅。

eB-Patrol 提供主動式防禦，來對抗今日不斷演變的混合式網路安全威脅。只要偵測到異常的變更，eB-Patrol 便立即回復被篡改的內容、發出警訊、執行指定程式、查詢可疑網路 IP 的來源、收集相關資料，以作日後分析及調查。eB-Patrol 提供與防火牆及入侵偵測系統等互補的機制，是系統管理者面對內、外部入侵的最佳解決方案。

### 產品應用

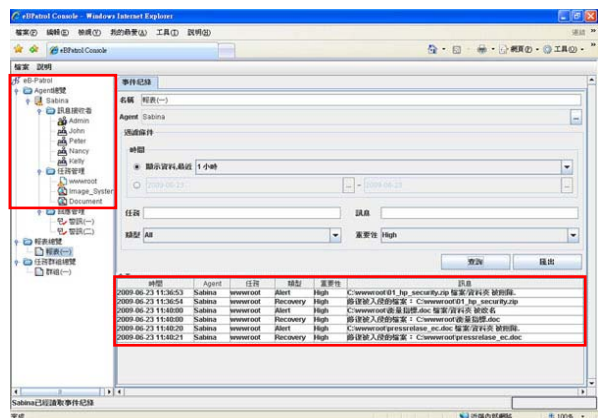
eB-Patrol 可保護重要的網站內容，免於：

- 駭客入侵篡改；
- 被加掛木馬程式，竊取機密資料；
- 病毒入侵所造成檔案的破壞；
- 人為的篡改（重要檔案遭員工意外變更）。

eB-Patrol 能同時偵測檔案及目錄層面，保護所有網站的內容（包括網頁、executables、scripts、applets），一旦偵測到任何未經授權的變更、加掛及刪除，便立即啟動回復與警訊。eB-Patrol 增強主動式安全防護能力，確保網站重要內容的可用性。而且，eB-Patrol 能查詢可疑網路 IP 的來源，並收集相關資料，備存入侵檔案，以作日後分析及調查。

### 產品效益

- 主動式防衛  
提供24x7即時偵測，不論是何種的篡改方式，eB-Patrol 都能立即復原被變更的內容，並與防火牆及入侵偵測系統進行互補，成為網站安全的最後防線。
- 智慧型控管  
提供嚴密的網站更新控管機制，允許使用者隨時更新檔案，而不需停止防護，確保網站內容時時刻刻都受保護。
- 網路遠端集中管理  
系統管理者能透過 IE 瀏覽器，隨時隨地從遠端進行設定，並集中控管多台受監測主機。
- 提昇管理效率  
提供監測任務群組管理，可輕鬆控管分散的檔案，有效節省維護管理的時間。
- 入侵蒐證機制  
可把入侵的資料(被篡改後的網頁、security logs等)保留下來，作為日後的分析及追蹤的證據。



系統管理者可透過 IE 瀏覽器隨時隨地進行監控：

1. 入侵發生時，即時在 console 上顯示警訊（聲音、圖示）；
2. 核對作業系統上異常的刪除動作。

# PROACTIVELY PROTECT YOUR SYSTEM

產品功能特色		標準版	專業版	
偵測	觸發式偵測	√	√	
	輪詢式偵測	√	√	
	偵測檔案的刪除及變更	√	√	
	偵測目錄中任何檔案的刪除及變更 (如被變更為木馬程式)	√	√	
	偵測目錄中任何檔案的新增 (如木馬程式的置入)	√	√	
警示與復原	即時自動回復被篡改的內容	√	√	
	文字模式警訊 (Email、SMS...)	√	√	
	其它模式警訊 (Audio、Visual...)		√	
	即時執行指定程式 (如掃毒程式...)		√	
	依不同檔案群組，通知各負責人。	√	√	
報表	監控情況報表	√	√	
	警示事件報表	√	√	
	可轉存 XML 格式	√	√	
	自動寄送每日報表	√	√	
	報表可排序及篩選，便於找出重大安控事件。	√	√	
			√	√
系統管理	提供 Web-based 遠端管理，以便進行防護管理。	√	√	
	所有內部通訊皆透過 SSL (Secure Sockets Layer) 加密傳輸	√	√	
	對多台伺服器提供中央控管功能。		√	
	智慧型檔案更新機制，透過授權的 IP 進行網站更新，而不需中斷監控。		√	
	查詢可疑網路 IP 的來源		√	
	入侵蒐證機制	√	√	
	依部門 或 application 分類管理檔案群組 (task management)。	√	√	
	提供監控任務群組管理 (task group management) 的功能，可跨伺服器定義任務群組，簡化管理操作。		√	
			√	√
	中文圖形化管理介面	√	√	

## 系統需求

eB-Patrol 專業版	
<b>Control Center</b>	
CPU :	Intel Pentium III 550 或以上
記憶體 :	64 MB RAM
磁碟空間 :	150 MB 加上儲存日誌所需的磁碟空間。
支援平台 :	MS Windows 2008, 2003, 2000, XP, Linux [Kernel above 2.6.13] (Red Hat Enterprise Linux, Fedora)
支援瀏覽器 :	IE, Firefox (with JRE 6.0)
<b>Agent</b>	
CPU :	Intel Pentium III 550 或以上
記憶體 :	128 MB RAM
磁碟空間 :	60 MB 加上檔案備份與儲存日誌所需的磁碟空間。
支援平台 :	MS Windows 2008, 2003, 2000, XP, Linux [Kernel above 2.6.13] (Red Hat Enterprise Linux, Fedora)

eB-Patrol 標準版	
CPU :	Intel Pentium III 550 或以上
記憶體 :	512 MB RAM 或以上
磁碟空間 :	200 MB 加上檔案備份與儲存日誌所需的磁碟空間。
支援平台 :	MS Windows 2008, 2003, 2000, XP, Linux [Kernel above 2.6.13] (Red Hat Enterprise Linux, Fedora)
支援瀏覽器 :	IE, Firefox (with JRE 6.0)

以上所有規格如有更動恕不另行通知。

## How does eB-Patrol work

