IBM ISS 威脅降低服務 – 端點系統保護 – 伺服器防護

產品特色

- ***專用來防護多種攻擊，包括這些透過加密 Web 交易進行的通道作業***
- ***整合多種檢驗技術，可深入各個網路層次提供優異保護***
- ***透過廣泛監視來確保資料機密性，同時簡化法規遵循工作***
- ***透過集中安全管理與延伸支援多種作業系統，來降低成本與複雜性***
- ***協助您實現虛擬化的好處***

深化您的防禦策略

儘管已設置防火牆和防毒保護，每年每兩家組織中就有一家經歷嚴重的安全侵害（而每次侵害都造成 660 萬美元的成本支出）。[1] 而當作業系統與應用程式修補程式試圖防堵連續不斷的攻擊時，駭客卻透過 Web 應用程式盜取更多的機密資料，這可以從 Web 攻擊數目呈指數成長看出端倪。內部安全漏洞（無心或故意）一直都是安全危害的潛在來源。

有 IBM Internet Security Systems™ (ISS) X-Force® 研發團隊支持的 IBM Internet Security Systems – 伺服器防護，可提供多層入侵防護與偵測，透過廣泛的監視、記錄與審核功能，協助您的伺服器避免受到為數日增的攻擊方法所害，同時徹底管理法規遵循問題。

在以下兩種實證產品中已啟用 IBM ISS - 伺服器防護：IBM Proventia® Server Intrusion Prevention System (IPS) 與 IBM RealSecure® Server Sensor。上述每一種產品都支援廣泛的作業系統，並提供穩固的安全防護以對抗為數眾多的攻擊，包括拒絕服務、遠端木馬攻擊程式、SQL Injection 與跨網站 Scripting。

通訊協定分析模組 (PAM) 技術

IBM 通訊協定分析模組 (PAM) 可推動安全整合，提供凌駕傳統 IPS 之上的網路與伺服器保護。

在保護伺服器的同時，維持伺服器最大的產量與執行時間

安全防護是細節的整合 (Sum of its pats)。不同於其他的伺服器防護解決方案，IBM ISS - 伺服器防護提供深度封包檢驗，這是其六層安全防護當中的一層。關於封鎖功能，Proventia Server IPS 與 RealSecure Server Sensor 提供：

- ***防火牆*** *- 可為您減少來自握有資源的、外部的駭客與來自內部（這些人可能瞄準您的安全漏洞）的威脅數目，從而掌控一切。*
- ***入侵預防系統*** *- 使用多層防禦來提供準確且強制執行的系統、網路、應用程式層與內部威脅防護。*
- *IBM Virtual Patch® 技術可協助預防已知與未知的攻擊，無論是否已發出安全漏洞修補程式。*
- ***緩衝區溢位防禦 (BOEP)*** *可協助預防已知與未知的緩衝區溢位安全漏洞遭到利用。*
- ***應用程式黑名單與白名單*** *- 協助您強制執行應用程式原則，以降低未授權的應用程式執行數目，從而減少伺服器曝露在惡意活動的機會。*
- ***安全 Web 交易檢驗能力*** *- 在交易遞送到 Web 應用程式之前執行檢驗。*

IBM ISS - 伺服器防護功能特別提供通訊協定分析模組 (PAM)，這是一種深度封包檢驗引擎，也是所有 IBM ISS 安全技術的核心。整合多種檢驗技術的 PAM 遠超越其他的伺服器防護解決方案，因為 PAM 可提供綜合且主動的防禦。再者，IBM ISS - 伺服器防護可緊密整合您現有的 IT 基礎架構，以便在不干擾的情況下保留合法的傳輸流程，讓您的業務能夠順暢營運，同時運用惡意軟體遞送防護來隔離您的資料。

簡化資料機密性與遵規測量

為了協助您管理標準與法令遵規，例如美國支付卡行業 (PCI) 資料安全標準 (DSS) 與美國健康保險便利及責任法

案 (HIPAA)，以及內部安全標準，IBM ISS – 伺服器防護納入四種監視：

- ***系統完整性監視*** – *警示您使用者與作業系統及應用程式的互動，並提供哪些人登入、採取哪些動作以及何時登出等資訊。*
- ***檔案完整性監視*** – *協助您監視使用者與機密檔案及資料夾的互動，以因應繁多的資料完整性標準，如美國沙賓法案。此技術的主要用途為偵測系統竄改，以及監視機密資料存取。*
- ***登錄完整性監視*** – *可以協助您監視及記錄對登錄機碼採取的成功或失敗動作，針對管理與使用者行為建立鑑識追蹤（對部分標準的報告來說是必要的）以處理潛在的漏洞點，然後藉由這些方式來因應資料完整性標準。*
- ***第三方監視*** – *可協助追蹤由第三方應用程式觸發，但可能是安全威脅的事件。*

此外，IBM ISS – 伺服器防護整合防毒強制執行，以確保伺服器接收最新的防毒更新項目，並報告未遵規的伺服器。Proventia Server for Microsoft® Windows® 是 NSS Labs 認證的主機入侵防護系統 (HIPS) 與 PCI 遵規。

跨廣泛作業系統簡化安全防護

IBM ISS – 伺服器防護專門用來提供入侵防護，以及跨廣泛企業作業系統（包括 Microsoft Windows、Linux®、IBM AIX®、UNIX®、Solaris 和 HP-UX）執行偵測。在此同時，本產品還透過 IBM Proventia Management SiteProtector® 系統的安全裝置、原則、事件分析、警示與工作流程，提供您簡易且具有指引的整體解決方案控制。您可以透過單一介面監視、分析、調整與產生報告，完全不用耗費時間與金錢在部署與學習多重管理工具。

透過虛擬化彙整 IT 作業

IBM ISS – 伺服器防護為虛擬環境就緒，可協助獲取伺服器虛擬化所提供的投資報酬 (ROI)，同時協助維護伺服器與作業系統層次的安全。

以虛擬機器為核心的防護可針對安裝 HIPS 代理程式的虛擬機器，分析進出其中的網路資料流量，進而保障虛擬網路通訊之間的安全。另一個重要優點是支援行動性，本產品可維護持續保護，同時藉由虛擬機器進行傳輸，彷彿傳輸是在實體主機之間進行。IBM ISS – 伺服器防護專門用來提供連續的安全防護，可支援下列環境：

- *VMware ESX*
- *Windows Server 2008 Hyper-V*
- *IBM Power Systems™ 邏輯分割區 (LP) 與工作量分割區*
- *Hewlett-Packard vPars 和 nPars*
- *Solaris Container*

爲何選擇 IBM？

IBM ISS – 伺服器防護由世界知名的 X-Force 團隊支持，該團隊負責維護世界上最為綜合的安全漏洞資料庫，許多搶先駭客一步的安全防護解決方案開發都採用其研究與威脅分析。IBM 的諮詢服務與技術嫻熟的服務專家，可協助您進行解決方案評估、設計與部署，或其他更多的綜合性管理。IBM 受管理防護服務 (Managed Protection Services，MPS) 提供即時、全天候防護與恢復運作、專家管理，跨各種平台與作業系統監視重要伺服器裝置，並升級呈報。

更多資訊

如需進一步瞭解 IBM ISS - 伺服器防護，請聯絡 IBM 業務代表或 IBM 事業夥伴，或造訪下列網站：

ibm.com/services/security

台灣國際商業機器股份有限公司
110台北市松仁路7號3樓
市場行銷處：0800-016-888按1
技術諮詢熱線：0800-000-700

台灣印製
2010 年 4 月

IBM 保留隨時變更規格或產品資訊的權利，恕不另行通知。本出版品可能會有技術上或排版印刷上的訛誤。IBM 僅以「現狀」提供本出版品，而不提供任何明示或默示之保證或條件（包括但不限於可售性或符合特定效用的保證或條件）。有些管轄區在某些交易上不允許排除上述保證，在這種情況下該項排除無效。使用本文資訊的風險由讀者自負。本文資訊若有變動恕不通知。IBM 可能會隨時改進及／或變更本文所述之產品和／或軟體，恕不另行通知。

本文件所提供之 IBM 與非 IBM 產品與服務的所有效能資料，都是在特定的作業與環境條件下取得。任何團體實作之後所獲得的實際結果，根據眾多因素的不同，特別是客戶的作業環境，產品或服務可能會有很大的差異。IBM 並不表示安裝任何此類產品或服務皆能獲得如此結果。

本文件所含之任何有關第三方的資料，皆根據取自於該方之資訊，我們不曾獨立驗證這類資訊的正確性。因此本文件並非明示或默示 IBM 建議或支持使用任何第三方的產品或服務。

[1] CSI/FBI 電腦犯罪與研究調查以及 Ponemon / PGP：美國資料外洩成本研究。