IMPERVA®
Protecting the Data That Drives Business®

網站應用程式防火牆

保護您的關鍵Web應用程式

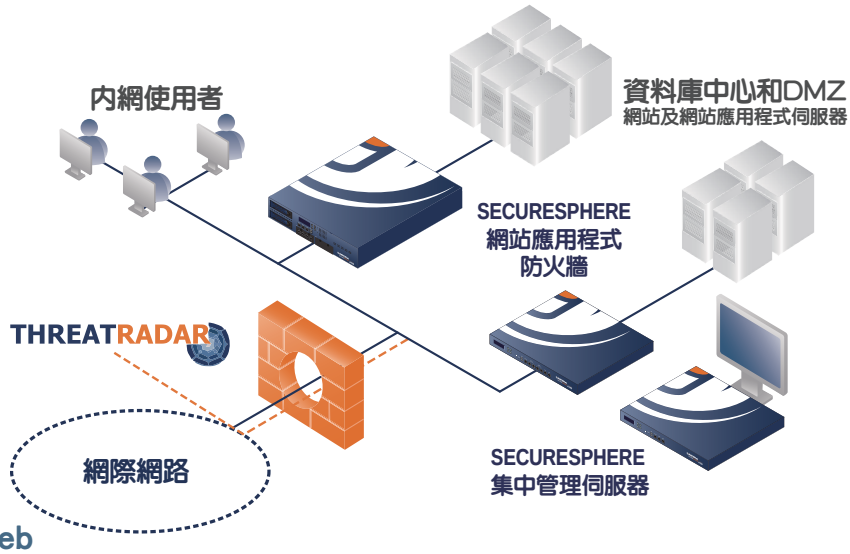
以業界領先的Web應用程式防火牆來保護Web應用程式免受攻擊和資料破壞。SecureSphere可幫助企業：

- 監控和保護Web應用程式
- 直接做到符合PCI 6.6的規定
- 透過動態建模技術達到自動化的維運安全
- 透過虛擬修補程式達到透通地保護Web應用程式
- 提供低延遲、高效能與企業級的管理和報表功能

SecureSphere 網站應用程式防火牆
全球威脅即時防護 信譽評等服務
全球威脅即時防護 防止詐騙服務

領先業界的Web應用程式安全方案

SecureSphere®Web應用程式防火牆可保護Web應用程式免受複雜的攻擊，阻止線上身份竊取，並防止資料經由應用程式洩露。包括layer 2 Bridge、Proxy和Non-Inline方式在內的多種設定選頂使部署變的非常簡單，而且不需要對現有應用程式或網路進行任何更改。因為有了領先業界的Web應用程式防火牆，所以比起任何其它同類產品，更多企業願意選擇Imperva來監控和保護其關鍵Web應用程式。Imperva SecureSphere為您的業務提供切實可行而且高度安全的解決方案，確保您的Web應用程式和資料安全無憂。



精確地監控和保護Web應用程式

SecureSphere Web應用程式防火牆採用多層檢查和多重安全防護來提供最安全的保護。

HTTP協定驗證

HTTP協定驗證可以防止包括緩衝區溢位、惡意編碼、HTTP偽裝以及非法伺服器操作在內的協定濫用。彈性的規則讓使用者可以嚴格遵守RFC標準，同時支援各種靈活多變的應用程式。

防止資料洩漏

SecureSphere檢查伺服器回應資訊以識別潛在的敏感資料（如持卡人資料和身份證字號）洩漏。除了報告在應用程式中何處發現了敏感資料外，還可以選擇讓SecureSphere阻止這些資訊從企業網站洩漏。

網路及平台防護

SecureSphere針對Web伺服器弱點、中繼軟體弱點和平台弱點中的已知攻擊提供廣泛的保護，這些已知攻擊的資訊來源是Imperva應用防禦中心(ADC)提供的超過6,500個特徵碼。ADC特徵碼不僅包括Bugtraq、CVE®和Snort®來源發現的攻擊，而且還包括透過ADC研究發現的威脅。SecureSphere還可透過檢測和識別Web蠕蟲獨特的特性組合來抵禦零時差的新Web蠕蟲攻擊。

SecureSphere的狀態式防火牆對來自外部和內部的非法使用者、協定和網路的攻擊提供保護，同時遵循安全規定的最佳做法，阻止非必要的協定觸及敏感Web應用程式。

無與倫比的準確度

Imperva獨特的關聯攻擊驗證技術，可準確識別最複雜的攻擊。個別違規可能無法明確地瞭解攻擊行為。但是，透過獨特關聯的違規組合就可以毫無疑問地確認攻擊。

Web 2.0和Web服務保護

SecureSphere透過動態學習Web 2.0和Web服務的行為來保護這些應用。學習的內容包括XML檔、元件、屬性、架構、變數和簡單物件連結協定(SOAP)。SecureSphere將識別並阻止任何嘗試竄改正常Web服務的行為。它還會抵禦Web 2.0應用程式中常見的威脅，包括SQL注入、XSS、CSRF和許多其他威脅。

自動化安全操作

自動應用學習

SecureSphere獨特的動態建模技術可自動學習被保護Web應用的結構、元件和預期使用模式。動態建模持續自動檢測有效的應用程式修改並將其納入應用程式行爲模型中。透過對比Web請求與行為模型，SecureSphere能夠精細的檢測不可接受的行爲並防止惡意活動。

應用程式使用者追蹤

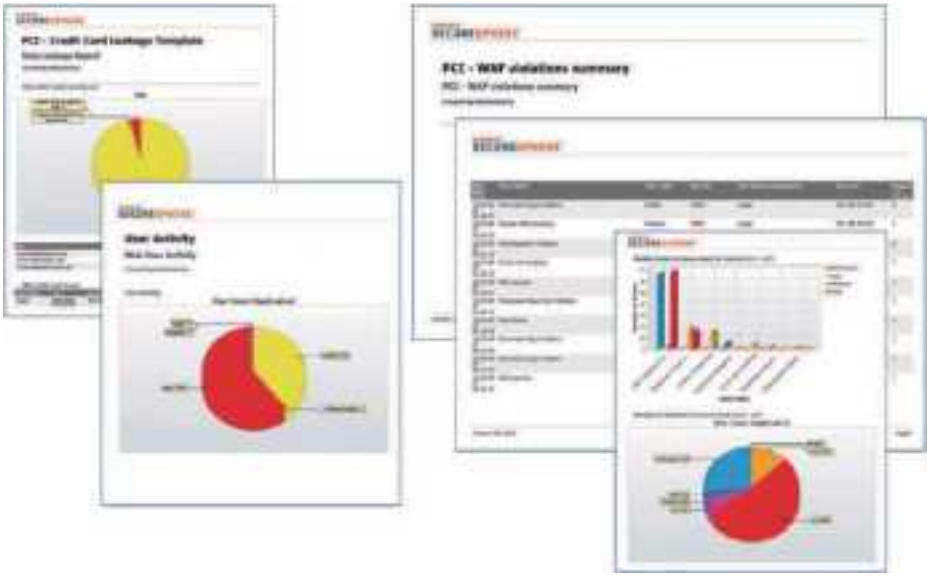
SecureSphere使用動態建模技術自動獲取Web應用的使用者名稱並將所有後續會話活動與這個使用者名稱的關係連接在一起。因此SecureSphere能夠獨一無二地按使用者監控、實行策略和進行稽核。

來自ADC的最新安全解決方案

Imperva ADC是一個國際知名的安全研究機構，該機構持續調查全球各地報告的新漏洞，分折來自眾多不同網站的非法探測流量，並進行根本性漏洞研究來識別最新威脅。這項研究的結果就是提供SecureSphere各設備的最新防護措施，包括特徵碼更新，協定驗證規則和關係連接規則。

SecureSphere 可防禦眾多應用程式攻擊，包括：

- Web, HTTPS (SSL) 和XML的弱點
- 資料隱碼 (SQL Injection)
- 連線截奪 (Session Hijacking)
- 跨網站攻擊 (Cross Site Scripting (XSS)
- 表單範圍的蓄意破壞 (Form Field Tampering)
- 已知蠕蟲 (Known Worms)
- 強力入侵 (Brute Force Login)
- 釣魚程式 (Phishing)
- 零時差的網路蠕蟲 (Zero Day Web Worms)
- 緩衝區溢位 (Buffer Overflow)
- Cookie 中毒 (Cookie Poisoning)
- 阻絕服務攻擊 (Denial of Service)
- 非人工的惡意入侵 (Malicious Robots)
- 參數值之竄改 (Parameter Tampering)
- 資料摧毀 (Data Destruction)
- 惡意內碼竄改 (Malicious Encoding)
- 跨越目錄存取 (Directory Traversal)
- 網路伺服器和平台攻擊 (Web Server and Platform Attacks)
- 網站間偵 (Site Recon)
- 作業系統命令植入攻擊 (OS Command Injection)
- 商業間諜 (Corporate Espionage)
- 匿名代理伺服器弱點 (Anonymous Proxy Vulnerabilities)
- 跨站冒名請求 (Cross Site Request Forgery (CSRF)
- Google 駭客入侵 (Google Hacking)
- 遠端檔案概括式攻擊 (Remote File Inclusion Attacks)
- 非法內碼竄改 (Illegal ding)
- 信用卡資料洩密 (Credit Card Exposure)
- 病患資料外洩 (Patient Data Disclosure)



PCI 6.6相關要求

SecureSphere Web應用程式防火牆可幫助成千上萬企業機構滿足PCI 6.6的 要求，這些企業機構包括電子商務、零售業、銀行、教育單位、科技業和博彩公司。

SecureSphere包含300個以上內建的報表，可自動符合法規要求，包括PCI在內。SecureSphere提供業務相關報表，因此工程、業務單位主管和PCI稽核員可以按各自的特定要求查看相對應的報表。

使用非入侵式的部署

不需要更改網路或應用程式

SecureSphere在業界所有Web應用防火牆中提供的建置部署選項最多，包括不需要更改任何網路或應用程式的透通橋接建置部署項目。

SecureSphere提供每秒數GB的傳輸量、數萬次的交易處理量，同時還能將延遲時間保持在低於毫秒的等級。

» 透通的橋接-部署簡單，在同類產品中性能最佳
» 網路路由方式-用於網路分段、路由和網路位址轉譯
» 反向代理-用於內容修改，例如：cookie簽送、URL改寫
» 透通代理-用於快速部署內容修改，不必更改網路
» 旁路監控-零風險監控和分析

高可用性

SecureSphere支援廣大範圍的高可用性選項：

» Imperva 高可用性(IMPVHA) - 提供極短時間內的故障復原
» 虛擬路由器備援協定(VRRP) - 提供路由器或代理伺服器部署力式
» (Active-Active) 及 (Active-Passive Redundancy) - 透過外部設備的備援機制
» 開放旁路(Fail-Open)的介面 - 提供單一閘道可用性
» 非置入性部署 - 針對零風險監視和檢測

提供企業級的集中管理

支援分散式部署

SecureSphere可以作爲獨立設備進行部署，也可以進行擴展以保護大型或分散式資料中心。SecureSphere MX管理伺服器提供集中式配置、監控和報表基礎架構，以便從單一控制台管理多個設備和安全政策規則。

同等級產品最佳監控和報表功能

即時集中展示頁面提供一個高階的系統狀態與安全事件圖形。可以很方便地對告警進行搜尋、排序，還可以直接將其連結到相對應的安全規則。

SecureSphere提供了豐富的圖形報表功能，使客戶能夠很輕鬆地瞭解安全狀態並符合法規要求。SecureSphere提供了預設的報表，也提供了基於Web應用下全面可客製化的報表。可以按需求查看報表，也可以每日、每週或每月透過電子郵件發送報表。

階層式管理

透過階層式的組織分組、細分管理權限和獨特定向的工作流程，大型企業環境和ASP環境的管理將得到簡化。

整合第三方(3rd Party)應用程式

SecureSphere整合大型企業應用的Web應用程式防火牆的整體安全活動。這包括領先的SIEM和日誌管理解決方案、基於角色進行身份驗證和用於弱點評估的Web應用掃描解決方案。

實施準確保護和自動化規則設定的動態建模(Dynamic Profiling)

準確實施Web應用安全措施需要瞭解無數不斷變化的變數，包括URL、參數、表單欄位和cookie等。Imperva已申請專利的創新性動態建模技術可自動建立所有Web應用元件的行為模型並設定可接受使用者行為的基準。透過構建應用使用情況的準確行為模型或「白名單」，動態建模簡化了監控和安全規則設定的工作，不需要大量手動設定或調整。此外，SecureSphere持續自動檢測有效的應用程式修改並將其納入到應用行為模型中。動態建模還可以產生應用的完整行為模型報表，其中包含真實使用情況統計資訊，可用於稽核實際應用使用情況是否符合預期。

SecureSphere 產品特色及設備規格

Web安全
» 動態建模（白名單安全方案）
» Web 伺服器與應用的特徵碼
» HTTP RFC 符合性
» 信譽評等為基礎的安全(Reputation based security)技術及IP國家所在(IP GeoLocation)
» 編碼資料標準化（Normalization of encoded data)
» 自動化機器/軟體

應用程式攻擊阻擋
» OWASP Top 10
» SQL Injection
» Cross Site Scripting
» Cross Site Request Forgery
» 請參見第 2 頁的防禦攻擊列表

HTTPS/SSL檢查
» 被動解密或終結會話
» 可選購 HSM 來儲存 SSL Key

Web服務安全
» XML/SOAP 行為模型執行
» Web 服務特徵碼
» XML protocol conformance

防止網路詐騙
» 詐騙及惡意軟體偵測

內容修改
» URL 改寫與模糊化
» Cookie 簽章
» Cookie 加密
» 客製化錯誤訊息
» 錯誤代碼處理

平台安全
» 作業系統入侵特徵碼
» 已知的和零時差蠕蟲安全對策

網絡安全
» 狀態監控防火牆
» 防DoS分散式攻擊

進階應用保護
» 關聯性規則包含了所有安全要素（白名單、黑名單），能夠檢測複雜的多階段攻擊

防止資料洩漏
» 信用卡號
» PII (Personally Identifiable Information)
» Pattern matching

規則/特徵碼更新
» 每週進行或者在出現嚴重威脅時可立即進行安全更新

身份驗證
» 所有身份驗證方法都可透通性的支援並可以bridge和non-inline監控模式檢查。可在Proxy模式下主動驗證用戶身份。
» 支援 RSA Access Manager 來進行雙因素身份驗證
» 支援 LDAP (Active Directory)
» 支援 SSL 用戶端認證

使用者辨識
» 自動追蹤 Web 應用使用者

部署模式
» Transparent Bridge (Layer 2)
» Router/NAT (Layer 3)
» Reverse Proxy and Transparent Proxy (Layer 7)
» Non-inline Sniffer (Monitoring only)

管理方式
» Web 使用界面 (HTTP/HTTPS)
» CLI 命令列界面 (SSH/Console)

管理
» 用於集中控管的 MX Server
» 整合管理選項 (X2000, X2500, X4500)
» 階層式的管理群組

記錄/監控/報表
» 即時儀表板
» 整合式圖形報表 (PDF、CSV格式)
» SNMP
» Syslog
» Email

高可用性(High Availability)
» IMPVHA (Active/Active, Active/Passive)
» Fail-open interfaces (bridge mode only)
» VRRP
» STP and RSTP

整合第三方(3rd Party)企業應用
» SIEM/SIM tools：ArcSight, RSA enVision, Prism Microsystems, Q1 Labs, TriGeo, NetIQ
» Log Management：CA ELM, SenSage, Infoscience Corp.
» Web application vulnerability scanners：WhiteHat, IBM, Cenzic, NT OBJECTives, HP, Qualys, and Beyond Security

TCP/IP Support
» IPv4, IPv6

加值經銷商

GSS 叡揚資訊

台北總公司：10461台北市中山區德惠街9號5樓
TEL：+886-2-2586-7890 FAX：+886-2-2586-8787
高雄辦公室：80453高雄市明華路317號6樓
TEL：+886-7-586-6195
海外據點：上海 營業範圍：兩岸三地及日本
www.gss.com.tw