Symantec
A Division of Broadcom

解決方案簡介

網頁安全服務--WSS
(Web Security Service)

快速一覽

網頁安全與威脅防護

- 由頂尖雲端服務平台所提供基於先進代理 (Proxy) 架構的安全服務，保護網頁存取與雲端應用程式的流量，用戶和設備
- 使用創新的網頁隔離--遠端瀏覽技術，來阻止針對網頁瀏覽器的威脅
- 使用具有風險等級情報的進階威脅情報資料以及惡意程式掃描引擎和沙箱功能，以阻止隱藏在加密流量中的惡意程式
- 使用 Cloud Firewall Service 預防非網頁類型威脅

實現雲端資料防護，強制執行政策控制

- 使用基於雲端或本地的資料外洩預防 (DLP) 選項
- 檢查 SSL 加密流量中的內容，以識別資訊安全違規情形並確保資料遵循性
- 設置雲端存取安全代理--Cloud Access Security Broker（CASB）政策，獲得對影子 IT 的能見度、套用雲端資料的監管、防禦威脅並且更輕易地確保遵循性

為Office 365提供安全性和效能

- 使用 Office 365 應用程式時，強制執行資料保護和威脅預防政策
- 自動更新政策以與 Office 365 基礎架構更改關聯 IP 地址更改保持一致
- 使用與 Microsoft 對等的雲基礎架構來提高效能

網頁安全雲端服務

企業對雲端應用程式的快速採用、網頁型態的應用越來越多的使用，這對現有的網路安全架構造成相當的壓力。漫遊用戶和新型的端點設備增加了額外的複雜性和挑戰。企業安全團隊必須在全新的時空背景下解決一系列問題，例如：

- 如何保護使用者（無論他們身在何處）免受形態不斷演變的威脅？
- 如何確保資料安全並符合法律規範？
- 如何有效管理新型裝置和行動／遠端用戶？
- 如何在不犧牲功能或靈活性的情況下將當前基礎架構遷移到雲端？

賽門鐵克網頁安全雲端服務--Symantec Web Security Service（WSS）是賽門鐵克整合式網路防禦平台 (Symantec Integrated Cyber Defense platform) 的關鍵元件，可以提供令人滿意的答案。它提供與領先市場的本地自建型安全網頁閘道：Symantec ProxySG 相同的主動型網頁保護功能，並以更富彈性及更高效能的雲端服務來提供。該服務位於員工（無論他們身在何處）與網際網路之間扮演代理互動角色，可保護企業免受網路威脅，並控制和保護企業對雲端應用程式和網頁的使用，防止機密資料外洩並確保對所有公司資訊和網頁／雲端存取的遵循性政策。

賽門鐵克網頁安全雲端服務 (WSS)，透過經認證的全球資料中心的多元化網路提供網頁和雲端存取安全性。通用政策實施（UPE）功能使管理員可以一次定義保護政策，並將其分發到所有網頁閘道。無論是在雲端中還是本地，企業都可以確保始終如一的保護措施。其一流的功能集，結合強大的整合解決方案選項，企業級網路安全功能和靈活的訂購價格模型，使 WSS 成為尋求在雲端交付服務中尋求企業級安全功能的公司的明智選擇。

特性與功能

賽門鐵克網頁安全雲端服務 (WSS)，強制執行精密存取控制和安全性政策，以按應用程式、設備、用戶或位置來管理網頁及網際網路使用情況。 包括以下先進技術所提供的企業等級功能。

網頁過濾和分類

- 每天處理超過 60 億個 網頁請求，並阻止數百萬次網頁攻擊和社交會工程詐騙
- 使用基於即時全球威脅情報的動態、即時網頁 (URL) 風險等級評比技術
- 將網址分類為 72 種內容類別中的一種或多種，其中 12 種安全類別（內定政策阻止的有 6 種），涵蓋 60 多種語言

進階的威脅防護

- 利用雙掃毒引擎及進階啟發式分析之類的多層偵測技術組合，阻擋惡意程式
- 利用自定義的白名單 / 黑名單功能和檔案信譽分析
- 使用威脅風險級別和地理 IP 位置情資自定義政策

通用連接，到處都一樣的連接性

- 廣布在全球資料中心的超大型架構，提供本地雲端存取的美好體驗
- 輕鬆連接筆電、行動裝置、防火牆、代理及更多……等

惡意軟體分析服務

- 利用進階分析（靜態代碼，YARA 規則，行為）以及連線威脅分析，即時檔案攔截功能來抵禦威脅
- 利用沙箱引爆可疑樣本並與網頁安全服務 (WSS) 協調以延遲檔案交付，直到分析完成

加密流量管理

- 攔截和解密 TLS ／ SSL 流量，以發現威脅和隱藏在加密流量中的潛在惡意內容
- 通過自我管理憑證，簡化客戶 PKI 管理

雲端防火牆服務

- 配置政策以阻止基於任何 TCP / UDP 端口的流量
- 根據已驗證的用戶／群組以及來源和／或目標條件設置政策（允許／拒絕）

網頁隔離服務

- 通過允許對未分類或潛在危險的網站，進行受保護的存取來提高員工的工作效率
- 通過基於風險級別的自定義隔離政策對員工存取控制進行優化微調
- 為高階主管和較高權限使用者提供安全的網頁瀏覽，並可以存取敏感資料與關鍵系統

雲端存取安全代理（CASB）

- 影子 IT 控制：通過識別正在使用的應用程式和服務來識別影子 IT，通過檢查數百個屬性來評估成千上萬（30,000+）個正在使用的獨特雲端應用程式的風險
- 不管受控管或非受控管端點所使用的任何雲端應用程式，均可以從賽門鐵克產品的統一事件檢視中加強能見度，以進行資料安全和威脅防護的搜尋、建立儀表板及報告

資料外洩預防（DLP）

- 使用市場上最先進的 DLP 比對和識別引擎，監視和保護行動裝置、本地和雲端中的敏感的資料；或將現有的本地 DLP 用於您的網頁／雲端流量
- 擴展 DLP 的覆蓋範圍，並可以直接查看和控制 60 多個雲端應用程式中的內容，這些應用程式包括 Office 365、Box、Dropbox、Google Apps 和 Salesforce……等

適用於分支機構和行動用戶的簡易入口

- 通過 Symantec Endpoint Protection 啟用全面的從網路到端點的多層次保護，從而簡化了行動裝置的應用程式的管理
- 與領先的 SD-WAN 解決方案整合

全面的安全性
可滿足當今企業的實際狀況

行動用戶、遠端辦公室以及雲端應用程式的採用，日益增加的法規遵循要求以及不斷發展的複雜威脅環境是企業 IT 和安全團隊必須面對的現實。 Symantec WSS 支持提供企業級功能來解決這些棘手問題，並確保網頁和雲端使用保持快速、有效、安全以及遵循。

世界上最大的民用威脅情報網路 - 賽門鐵克全球情報網路提供了久經考驗的代理技術，可確保即時防禦已知和未知的網路威脅。 通過廣泛的 Web--網頁和雲端應用程式控制、Web- 網頁隔離、惡意軟件掃描、資料外洩預防，CASB 服務以及詳細的報告功能，WSS 讓管理員可以建立和強制執行詳細的政策，這些政策可立即應用於所有涵蓋的用戶，無論他們位於何處， 包括固定位置和漫遊用戶。

賽門鐵克網頁安全服務--WSS：經過實證且深受信賴的全代理網頁加速及安全架構--ProxySG ，透過雲端服務來提供。

賽門鐵克網頁雲端服務 (WSS) 功能

威脅防護

- 由世界上最大的民用威脅情報網路提供支持（1.5 萬家企業、1.75 億用戶、3,000 名以上的研究人員）
- 已內建最佳實務政策
- 基於威脅風險級別的進階控制
- 網頁隔離 (Web Isolation) 能透過遠端瀏覽技術，隔離未分類及可能有風險的流量，以便在允許存取各種網頁的同時，防止惡意軟體和網路釣魚
- 提供非網頁型態的網路流量安全的雲端防火牆服務
- Symantec 內容與惡意程式分析--以多層檢查和可自訂的沙箱來偵測和封鎖規避傳統分析的進階威脅

可接受的使用控制

- 通過精細政策（按使用者、群組、位置等）進行網頁過濾
- 網頁應用程式攔截
- 雲端存取安全代理 (CASB) 查找和報告 *

資料外洩預防 (DLP)

- 可與賽門鐵克資料外洩預防 (DLP) 雲端服務整合
- 可與第三方資料外洩預防 (DLP) 整合，包含地端自建型的 DLP

報告和視覺化功能

- 可自定義的儀表板，並提供深入可抽絲剝繭的資訊
- 預先設定和自定義的報告
- 已排程的報告利於透過電子郵件傳遞觸發的警報

專為 Office 365 用戶打造的安全性和效能

隨著企業遷移到 Office 365 之類的雲端應用程式，傳統的網路架構已經發生了巨大變化。傳統上，來自遠端站點和行動用戶的流量通過公司資料中心連接以存取應用程式，並利用安全性基礎架構來存取網頁。 隨著組織遷移到 Office 365，此安全架構可能會增加延遲並增加成本。

企業可以放心依靠賽門鐵克網頁雲端服務--WSS (Symantec Web Security Service) 將其整個網路安全堆棧移轉至雲端服務，從而實現與雲和軟體即服務 (SaaS) 的應用程式（如 Office 365）的直接安全連接，從而以更低的成本受益於更快的安全性和網路架構。 該服務可以在存取 Office 365 時實施全套完整的控制，包括掃描 Office 365 流量中的惡意軟體和威脅，以及檢查加密的流量中的資料洩漏和違反資訊安全相關法規等行為。

賽門鐵克全球情報網路提供了網頁安全服務，以確保對 Office 365 應用程式的基礎架構所做的任何更新（例如 IP 位址的更改）自動與企業的 Office 365 安全政策保持一致，從而為我們的客戶實施一致的安全政策 。 此外，先進的內容互連和傳輸控制協議（TCP）連接加速功能可減少鏈接躍點 (hops) 並提高吞吐量，從而為客戶提供更高的效能和增強的用戶體驗。

賽門鐵克網頁雲端服務 (WSS) 功能（續）

SWG 日誌記錄管控

- 可依授權等級或位置來控制資料刪除
- 可配置的資料保留期（2 到 365 天）*

驗證

- 利用 Windows Active Directory（AD）無需更改
- 支持 SAML v2（發布和重定向綁定）

加密流量檢測

- SSL ／ TLS 加密流量攔截，解密和檢查的符遵循範
- 使用具有 Symantec PKI 託管的根和中級 CA 或客戶提供的 PKI 的安全 CA
- 服務器憑證頒發機構驗證與撤銷檢查

連接方式

- 通過 SEP、SEP Mobile 或 Unified Agent 為遠端／行動用戶提供安全的流量重新導向
- 不安全的代理存取
- IPSec 連接（PSK 和憑證方法）
- 強化代理（Windows 和 Mac 作業系統）*

雲端基礎架構

- 企業用戶可以使用的所有全球資料中心
- 區域資料中心可用於報告
- ISO27001 和 SSAE-16 SOC3 認證

連接方式		
IPSec VPN（站點到站點）：大多數支持 IPSec 的 Juniper、Cisco、Palo Alto、Fortinet 和 Checkpoint 防火牆 *		
來自 ProxySG 和其他代理設備的代理鏈接		
詳盡的代理		
Symantec Endpoint Protection（SEP）：SEP 14（14.1 RU1 MP1）或更新版本		
Symantec Endpoint Protection Mobile（SEP Mobile）：iOS 行動裝置		
SD-WAN 技術合作夥伴關係：與第三方 SD-WAN 解決方案提供商的經認證可進行交互操作的合作夥伴關係		
桌面連接器	WSS 代理 作業系統： ・64 位 Windows 10 專業版、企業版或教育版 1703 或更新版本 ・macOS 10.15 High Sierra 或 更 新版本 統一代理（v4 和更早版本） 作業系統： ・Microsoft Windows7(32位和64位)	最低硬體需求： ・必須滿足特定作業系統的最低硬體要求 ・ X86 或 x86-64 相容處理器 ・100MB 的可用硬碟空間用於軟體安裝和保留日誌 ・高速的網際網路連接
支持的身份驗證服務		
微軟 Active Directory，簡稱 AD	作業系統： ・Windows 2003 SP2 或更新版本 ・Windows 2008 SP2 或更新版本	最低硬體需求： ・必須滿足 Windows 2003 SP2 和更新版本的最低硬體需求 ・X86 或 x86-64 相容處理器 ・100MB 的可用硬碟空間用於軟體安裝和保留日誌 ・高速的網際網路連接

* 依所擁有的授權內容配置選項。
** 相關訊息，請參閱《部署指南》。

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的政策性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。
若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或
賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號
電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw