Symantec
A Division of Broadcom

解決方案簡介

Content Analysis
內容與惡意程式分析
進階的多層威脅防護

快速一覽

- 多層次安全性，可有效防禦已知和未知威脅。
- 一種獨特的多重檢測方法，可以快速分析可疑檔案和網頁鏈接(URL)，與正在運行的惡意軟體進行交互以顯現其完整行為，以及揭發零時差威脅和未知惡意軟體。
- 過濾，經由本地或雲端沙箱分析，可對真正未知檔案進行有效而徹底的檢查。
- 排定優先順序進行分析以減少SOC和事件響應團隊必須處理的警報數量。
- 可與Symantec Proxy代理平台，部署在相同的實體主機、虛擬環境或在雲端中部署，以提高投資報酬(ROI)和靈活性。
- 一種創新的多層次安全解決方案。
- 可與賽門鐵克和合作夥伴生態系統高度整合。

在網際入口以自動化、先進的多重防護技術，第一時間封鎖、檢測和分析避傳統分析的進階威脅

企業容易遭受到日益複雜的攻擊、暴險加劇，更需要最新的防禦思維與措施——它必須結合更有效的攻擊檢測、分析和回應技術相輝映。

Symantec ™ Content Analysis 使用全面的安全性方法，可提供無與倫比的保護，防止已知、未知和有針對性的目標攻擊。 與 Symantec ProxySG、Secure Messaging Gateway、Symantec Endpoint Protection、Security Analytics 或其他第三方工具搭配使用時，Content Analysis 採用分層方法來針對網路，郵件或端點流量進行威脅防護。Content Analysis 使用 Symantec 和其他領先的安全供應商來提供黑／白名單和檔案信譽服務、雙重反惡意軟體引擎、機器學習以及通過本機或雲端沙箱進行的深度檢查和引爆。總而言之，這種內容和惡意體分析的融合是針對目標惡意軟體攻擊的最佳保護。內容分析旨在保護組織免受網路，端點或目標電子郵件中的病毒、特洛伊木馬、蠕蟲、間諜軟體和其他惡意內容的侵害。

提供可擴充的內置威脅分析

複雜的攻擊被精心設計成有多種形式，以避免被各自為政的的單一功能安全系統偵測及攔截；沒有任何一種技術可以有效地阻止所有威脅。內容分析採用了不同的方法，並提供了一個用於多層次／多供應商威脅檢測和防護的平台，從而大大減少了安全營運中心 (SOC) 和事件回應團隊需要解決的警報數量。通過慎密整合網頁代理閘道--ProxySG、郵件安全閘道--Secure Messaging Gateway 以及內容分析--CAS：

- 在網際入口（閘道）第一時間阻止已知的惡意網頁連結 (URL) 和電子郵件
- 運用賽門鐵克檔案信譽服務 (FRS) 並進行廣泛的白名單／黑名單掃描
- 通過進階機器學習和靜態代碼檔案分析技術來分析未知檔案
- 業界唯一：可同時啟用 2 種知名防毒引擎掃描內容，以提高檢測精度 +12%
- 通過高度精密化且成熟技術的沙箱引爆未知檔案
- 具與多種常用安全系統完美整合能力，包括 Symantec Endpoint Protection，以提供端點可見性、更高防護力和快速回應

賽門鐵克檔案信譽服務

內容分析 (CAS) 會為其處理的每個檔案建立雜湊 (hashes)。 然後將這些雜湊值與 Symantec 基於雲的檔案信譽服務 (FRS) 分類進行比對，以識別已知檔案。 該服務使用信譽分數來表明文件是“已知”可信任檔案還是惡意檔案。然後，根據信譽積分，如果被判定為惡意，則將檔案阻止，如果被判定是安全的，則將檔案傳遞給用戶，或者使用防病毒掃描和沙箱進行進一步處理。Symantec FRS 實現了群眾外包、集體智慧的安全性--一名用戶在 Content Analysis 沙箱中引爆的任何檔案都與 FRS 服務共享，因此，如果該檔案出現在另一名 Symantec 用戶中，則該檔案將被阻止。

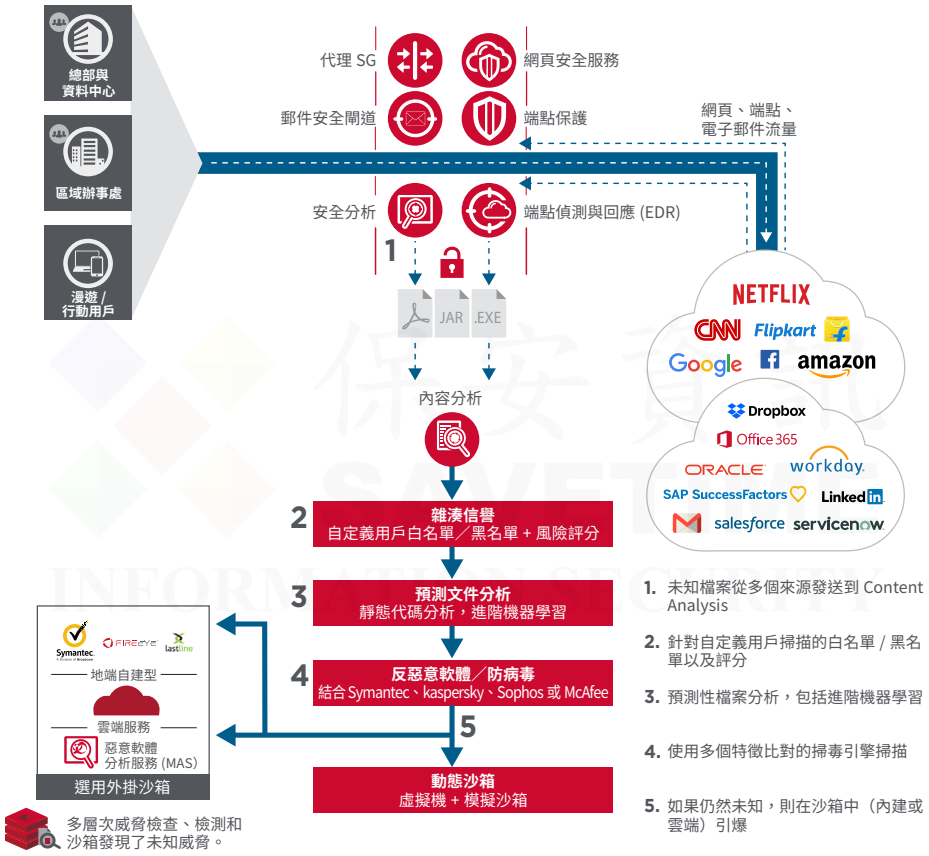
端點整合

Content Analysis 與 Symantec Endpoint Protection 和其他端點解決方案整合在一起。當沙箱分析確定該檔案是惡意時，Content Analysis 會查詢端點解決方案的主控台以確定網路中是否有任何工作站也受到感染。然後，該信息將包括在給管理員的報告中，並提供將檔案湊湊添加到黑名單或運行補救政策的選項，以防止整個組織受到更嚴重的感染。

CAS 的內容分析是業界少見的開放平台，允許博通 (Broadcom) 的賽門鐵克 (Symantec) 企業部門可以與其他領先技術供應商合作，以提供增強的保護。 最新的版次支持 Symantec，Kaspersky，Sophos 和 McAfee 等一線防毒軟體引擎，與僅安裝在用戶端的防毒軟體相比，它提供了更好的保護。 最多可以同時使用兩個防毒軟體引擎來改善檢測和阻止。 威脅檢測引擎包括：

- 檢查值校驗和簽名比對已知威脅檢查值
- 用於制敵機先的命令和控制 (C&C) 連線行為分析
- 用於深度腳本和可執行黨文件分析的模擬模式

圖 1：在 ProxySG 仔細檢查 Web 流量之後，Content Analysis 將基於哈希信譽，進階機器學習來分析該流量中的所有檔案，然後使用雙防毒軟體掃毒引擎掃描惡意軟體和病毒。所有剩餘的未知文件都將發送到動態沙箱。



靈活的配置可進行入站和出站的雙向流量分析，並包括以下選項：設置超時持續時間，如果檢測到錯誤則丟棄文件，即時沙箱以一路追溯至原發資安事端，以及定義受信任的站點。 設置白名單 / 黑名單（帶有擴展名）以及檔案大小和內容類型限制的政策。警報和日誌文件也可以自定義。 通過 Symantec Enterprise Licensing 可以在網關上使用此強大的進階威脅防護，以實現靈活的部署並滿足任何組織的需求。

部署選項包括：

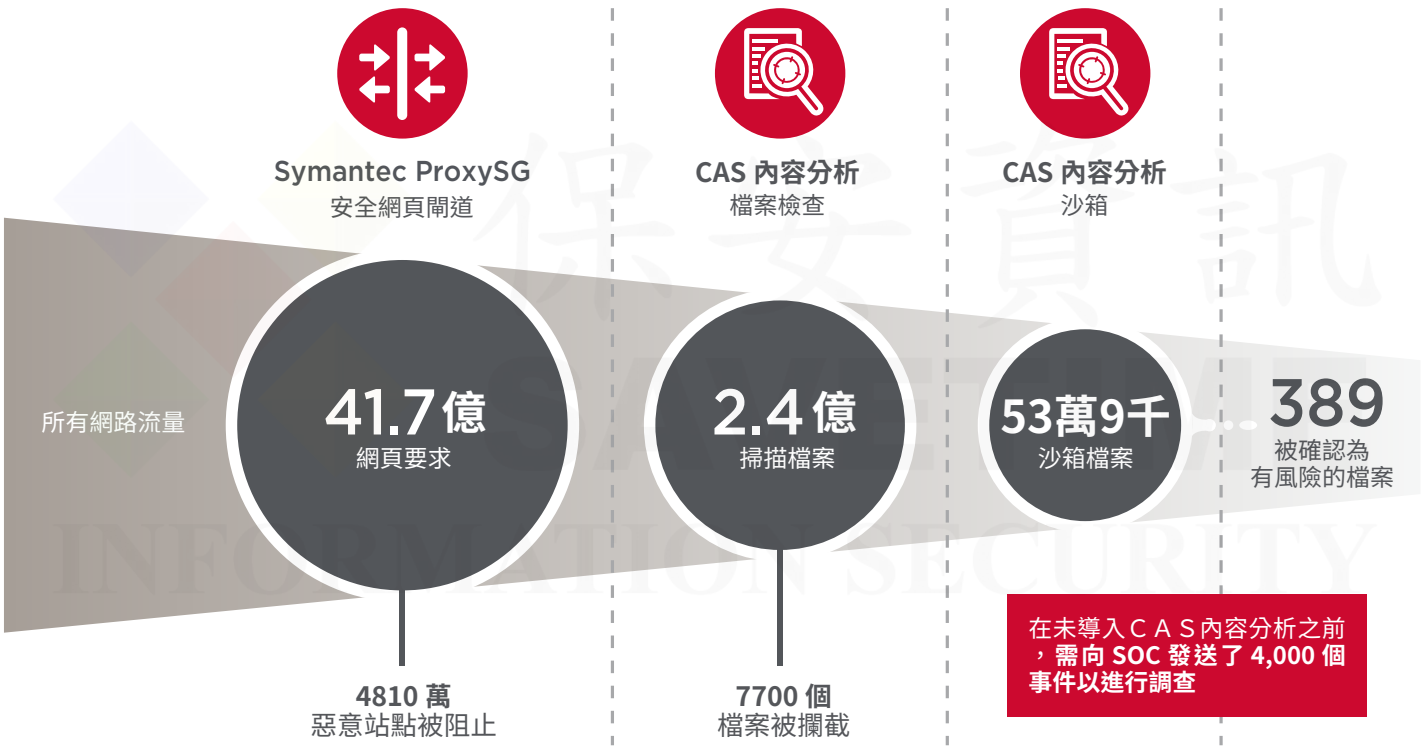
- 高效能的硬體主機，可滿足最大網路架構的嚴格要求
- 優化的虛擬設備可減少硬體主機成本，支持分支機構或在 AWS 等雲端環境中進行部署
- 雲端代管的 Web 安全和惡意軟體分析（沙箱）服務，提供領先業界的威脅防護

有效抵禦進階威脅

內容分析通過多元威脅情報來源來阻止有針對性的目標攻擊，並與領先的網頁代理 (Proxy SG) 和電子郵件閘道 (SMG)）架構整合在一起，以阻止惡意網頁瀏覽和電子郵件。通過多重安全檢查，以阻止惡意軟體進入您的組織。檢測並阻止更進一步的攻擊，甚至在最快的網路上也可以更好地管理威脅分析，並減少誤報。要獲得最強大的保護，就需要只有賽門鐵克才能提供的多層次高端技術且可以互相串連的安全平台。

某《財富》雜誌前二十大企業在 30 天內的真實網路流量內容

圖 2：在此示例中，Symantec ProxySG 網頁代理／分類過濾／和內容分析 (CAS) 使用多階段流程分析了數十億個 Web 請求，並將其篩選為僅少數有效警報，需要安全團隊進行進一步調查



內容分析實體主機選項

內容分析可以與 Symantec Proxy 部署在相同的 Secure Web Gateway 硬體主機上。

安全網頁閘道硬體裝置機型	SSP-S410-10	SSP-S410-20	SSP-S410-30	SSP-S410-40
平台規格				
系統				
中央處理器	1x10 core 2.2 GHz 4210 Cascade Lake	2x10 core 2.2 GHz 4210 Cascade Lake	2x16 core 2.1 GHz 4216 Cascade Lake	2x20 core 2.1 GHz 6230 Cascade Lake
記憶體	48 GB (DDR4 SDRAM)	96 GB (DDR4 SDRAM)	192 GB (DDR4 SDRAM)	384 GB (DDR4 SDRAM)
存儲固態硬碟	2x 480 GB	2x 960 GB	2x 960 GB	2x 1.9 TB
開機硬碟 (SATA)	2x 64 GB	2x 64 GB	2x 64 GB	2x 64 GB
電源供應器	2x 1200W	2x 1200W	2x 1200W	2x 1200W
網路介面--政策	10Gb 乙太網 (RJ-45) x 4	10Gb 乙太網 (RJ-45) x 4	10Gb 乙太網 (RJ-45) x 4	10Gb 乙太網 (RJ-45) x 4
網路介面--管理	1Gb 乙太網 (RJ-45)	1Gb 乙太網 (RJ-45)	1Gb 乙太網 (RJ-45)	1Gb 乙太網 (RJ-45)
可選用的網路介面卡	4 埠 10GB 乙太網 (RJ-45，具有旁路功能)、2 埠 10GB 乙太網 (RJ-45)、4 埠 1GB 乙太網 (RJ-45，具有旁路功能)、4 埠 10GB 光纖網 (LC，具有旁路功能)、2 埠 100GB 光纖網			
安全網頁閘道硬體裝置機型	**SSP-S410-10**	**SSP-S410-20**	**SSP-S410-30**	**SSP-S410-40**
機架規格				
包裝尺寸和重量				
寬度	610 mm (24.01 in.)	610 mm (24.01 in.)	610 mm (24.01 in.)	610 mm (24.01 in.)
總深度	995 mm (39.17 in.)	995 mm (39.17 in.)	995 mm (39.17 in.)	995 mm (39.17 in.)
高度（在托盤上）	290 mm (11.41 in.)	290 mm (11.41 in.)	290 mm (11.41 in.)	290 mm (11.41 in.)
毛重（磅）	~26 kg (57 lb)	~26 kg (57 lb)	~26 kg (57 lb)	~26 kg (57 lb)
實際尺寸及重量				
寬度	483 mm (19.01 in.)	483 mm (19.01 in.)	483 mm (19.01 in.)	483 mm (19.01 in.)
總深度	826.8 mm (32.55 in.)	826.8 mm (32.55 in.)	826.8 mm (32.55 in.)	826.8 mm (32.55 in.)
高度 (一個機架單元 U)	43.5 mm (1.71 in.)	43.5 mm (1.71 in.)	43.5 mm (1.71 in.)	43.5 mm (1.71 in.)
淨重	~22 kg (48.5 lb)	~22 kg (48.5 lb)	~22 kg (48.5 lb)	~22 kg (48.5 lb)
環境及電氣規格				
主輸入電源--PDU 配電盤	雙熱插拔備援電源，100 to 240 VAC, 7.08A, 47 Hz to 63 Hz			
設施電源接口	Type B, 5-15R, 120 VAC			
功率電源供應器輸出	1200W (Max)	1200W (Max)	1200W (Max)	1200W (Max)
熱功率	4096 英制熱單位 (BTU)	4096 英制熱單位 (BTU)	4096 英制熱單位 (BTU)	4096 英制熱單位 (BTU)
工作溫度（攝氏度）	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)
不工作時溫度	−40°C to 70°C (−40°F to 158°F)	−40°C to 70°C (−40°F to 158°F)	−40°C to 70°C (−40°F to 158°F)	−40°C to 70°C (−40°F to 158°F)
工作相對濕度	20% 至 85% 相對溼度 (Rh)	20% 至 85% 相對溼度 (Rh)	20% 至 85% 相對溼度 (Rh)	20% 至 85% 相對溼度 (Rh)
不工作時相對濕度	10% 至 85% 相對溼度 (Rh)	10% 至 85% 相對溼度 (Rh)	10% 至 85% 相對溼度 (Rh)	10% 至 85% 相對溼度 (Rh)
工作期間高度(海拔)	3,000 公尺	3,000 公尺	3,000 公尺	3,000 公尺
不工作時高度(海拔)	12,000 公尺	12,000 公尺	12,000 公尺	12,000 公尺

內容分析實體主機選項（續）

安全網頁閘實體主機		
規定	**安全生**	**電磁相容性**
國際	UL: UL 60950 1, 2nd Edition cUL: CAN/CSA C22.2 No. 60950 1 07, 2nd Edition CB: IEC 60950 1:2005 +A2:2013+ Summary with National Differences: EN 60950 1:2006+A2:2013	CISPR22:2008 Class A; CISPR32 Class A
美國	UL: UL 62368 1, 2nd Edition	FCC part 15, Class A /ANSI C63.4 2014
加拿大	cUL: CAN/CSA C22.2 No. 62368 1 14, 2nd Edition	ICES-003, Issue 6 Class A / CAN/CSA CISPR 22 10
歐洲聯盟(CE)	CB: IEC 62368 1:2014 (Second Edition) Summary with National Differences: EN 62368 1:2014+A11:2017	EN 55011, EN 61000 6 3, EN 55032, CISPR 32, Class A EN 61000 3 2 / EN 61000 3 3, EN 55024 / EN 61000 6 1, EN 61000 4 2 / EN 61000 4 3, EN 61000 4 4 / EN 61000 4 5, EN 61000 4 8 / EN 61000 4 11
日本	---	VCCI V-3, Class A
墨西哥	NOM-019-SCFI by NRTL 聲明	---
阿根廷	S Mark – IEC 60950-1	---
台灣	BSMI – CNS-14336-1	BSMI – CNS13438, Class A
中國	CCC – GB4943.1	CCC – GB9254; GB17625
澳洲／紐西蘭	AS/NZS 60950-1 第二版	AS/ZNS-CISPR32, AN/NZS CISPR 32:2015 + C1:2016 ED.2.0
韓國	---	KC – RRA, Class A, KN32/KN35, KN61000 4 2 / KN61000 4 3, KN61000 4 4 / KN61000 4 5, KN61000 4 6 / KN61000 4 11
俄羅斯	EAC - TP TC 004/2011	EAC - TP TC 020/2011
環保規範	RoHS-Directive 2011/65/EU, REACH-Regulation No 1907/2006	
產品保固	出貨日期起一 (1) 年有限且不可轉讓的硬體保固。 額外選購支援合約可供 24/7 軟體支援及硬體支援選項之用。	

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