預防是整合式端點安全解決方案能發揮最大效益的基石

作者
Adam Licata

白皮書

本中文化由保安資訊提供
https://www.savetime.com.tw

Symantec™
A Division of Broadcom

目錄

複雜度是端點安全的絆腳石

攻擊者會以節點作為目標--他們會檢查各裝置或網路聚集 (連接) 點，尋找它們何處有開放的弱點進而入侵你組織內的資源。你的環境越複雜，你就越有可能具有暴露出攻擊者可以攻擊的漏洞可供利用。這就是為什麼管理並保護所有端點既重要又困難的原因。

一般組織通常有數千甚至數十萬個要保護的端點。這些組織內的端點涵蓋各種不同外形尺寸 / 裝置類型 / 操作系統而且數量不斷成長，其中甚至有不少數量不受組織管理者直接控制。這些端點被用於存取各式各樣的資源，使用各種應用程式--主要 APP 商店中可用的 APP 數量[1]，到 2021 年，預估全球應用程式下載量將達到 3520 億[2]。

為了確保組織內的政策，安全性和合規性能夠被維護，所有這些端點都需要被管理和保護。管理和保護端點的工具理應幫你從一團混亂中整理出秩序，但結果可能適得其反，它們通常會加劇複雜性。Ponemon 發現一般組織平均在端點安裝了 7 種不同的代理程式以支援 IT 管理和安全[3]。

每個代理程式都獨自運行--每個都對同一個的執行緒或檔案做重覆載入檢查、掃描，這都會拖慢端點的速度。每種代理程式都必須個別部署，使用自己的主控台進行配置，管理和維護政策和排定升級。雖每個代理程式防護功能略有不同，但你都必須學習其運作的原理以及學習該如何整合入你現有的系統和工作流程。不難理解為什麼超過 75% 組織認為其端點安全解決方案既無效又困難且管理成本高昂[4]。

然後就是每個代理程式都提供特定但通常重覆的功能，例如網路防火牆、端點偵測和回應 (EDR)、裝置控管、惡意軟體防護，或其他能力。當然你可自行決定你最終要使用哪個代理程式。Ponemon 發現 47%的購買 EDR 解決方案的組織平均花費了 3 個月時間來部署，而他們只使用了全部功能中的 46%[5]。

追踪哪個代理程式正在做什麼會產生很多不必要的複雜性，進而產生更多錯誤和漏洞。代理程式發出的警示可能已經被另一個處理了。但不幸的是，這通常取決於你是否有追踪每個事件並驗證是否確實有處理該事件。所以當出現問題時，幾乎無法找出到底是哪個代理程式出錯。

是時候改變了。現在正是採取整合以達到端點安全的最佳時機。

完美的端點安全整合可以大大簡化你的環境並減少危險節點，避免疊床架屋的心力付出並簡化工作流程。當整合目標完成，它可以提供強大而有凝聚力的安全性，有效地保護你的組織並避免針對你端點的威脅 -70%的組織認知到在過去的一年裡新的未知威脅是有顯著增加[6]。此白皮書定義了真正的整合方法需要什麼，以及描述 Symantec 各產品如何達到此目標。

定義何謂端點安全的成功整合

整合向來都不是件簡單的事。不能僅僅因為某個層面說它是整合，它就是整合。要實現整合，需要從一開始就定義好你的需求。它必須深入到各個層面--產品、產品組合和生態系統：來建立單一、統一的點到點解決方案。讓我們來看看這需要什麼：

產品整合

把各產品功能整合到單一個解決方案中，將會減少採購、部署設定、管理和維護多種產品的成本，此效益是顯而易見的。但是，如果這些功能仍然需獨立運作，可以說根本沒有效益。真正的整合解決方案不僅是將功能整合到單一代理程式中，它還要可以確保這些功能在單一主控台下可緊密結合並整體協同運作。所有不同的功能必須能互相溝通，一次性處理各種情報，分享資料以確保正確識別威脅，適當處理事件，並優化政策以加強和保護內部環境免受未來類似事件的影響。你不再需要部署多種偵測技術也不再需手動關聯安全事件。各功能會自行溝通且自動化處理，因此動作可以簡化並最優化確保結果。

產品組合整合

當供應商說他們提供整合的產品組合時，重要的是深入解其真正意涵。解決方案不應只是將各品牌元素膚淺的組合在一起，而是它們應該要能真正合而為一。即使由多個不同的產品組合，你亦不再需要專精指令碼或程式開發來達到交換威脅情報和應對威脅的目標。能稱得上真正的整合

[1] “截至 2018 年第一季度，主要 APP 商店中可用的 APP 數量” Statistica，https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/。

[2] “APP 下載和使用情況統計情報（2018）”，Artyom Dogtiev，2018 年 10 月 8 日，應用程式業務，http://www.businessofapps.com/data/app-statistics/。

[34] “2017 年端點安全風險狀況”，Ponemon Institute LLC，2017 年 11 月，https://cdn2.hubspot.net/hubfs/468115/Campaigns/2017-Ponemon-Report/barkly-2017-state-of-pointpoint-security-risk-ponemon-institute-final.pdf。

[56] “2018 年端點安全風險狀況”，Ponemon Institute LLC，2018 年 10 月。

產品組合其看起來和操作就要像單一解決方案。它會自動處理和共享不同產品之間的情報，使一切都以有效率的方法運行，故出現需額外支援的機率，就微乎其微。它還需提供一個主控台，可以輕鬆管理和調整各項功能。如此一來整合的成本可最小化，並最大程度地提高所購買產品的價值。

生態系統整合

沒有單一供應商可保證可達到所有功能，尤其是在網路安全方面，因此能夠與其他供應商的解決方案整合非常重要。通常，這種整合是用供應商提供的應用程式介面 (API) 來相互溝通，該 API 允許其他供應商從其解決方案中輸出資料，以供自己產品的分析或其它目的。但這還不夠。真正有意義的整合是雙向溝通。供應商需要允許其系統中的輸入以及資料輸出，以確保一加一確實等於三！為了實現這一目標，供應商必須提供開放的 API，來讓其它供應商或開發人員都可以使用它們的商業版，現成或自訂應用程式存取。這些開放的 API 應該允許如下外部操作：

- 檢索安全事件以進行威脅關聯、優先權區分、產生事件和排定工作流程
- 上傳第三方威脅情報（例如：威脅來源或黑名單）以加強事件內容、威脅搜尋和主動預防（例如：STIX 開放標準就允許如此操作。）
- 管理業務流程、自動化和營運管理的政策，以進一步達成大型環境中的簡化
- 通過立即採取行動來應對威脅，例如：將檔案列入黑名單、隔離檔案、隔離端點、終止執行緒等（例如：OpenC2 開放標準就允許如此操作）

理想情況下，供應商將幫助建立一個客戶和合作夥伴社區，他們可以自由地交流想法並加速創新。這種類型的生態系統整合，可讓你的基礎架構以更緊密的方式運作，從而提供更高的效率和結果。

只有當解決方案可以支援產品、產品組合和生態系統這三個層次時，才可以真正將其稱為整合。只有將整合這一概念融合到所有內容中，你才能簡化端點管理和安全性，並最小化任何“接縫”，以建立和維護符合您所需的安全和合規性目標的安全立場。

賽門鐵克如何成功整合

賽門鐵克的整合方案提供了世界上最先進的單一代理程式端點安全解決方案，且各個安全引擎兼具廣度及深度防護。Symantec Endpoint Security 提供高級預防作為基本的核心保護，而其他終端安全產品組合的部分提供額外的保護，進而實現最完整的安全性，請參見圖 1 防護功能。額外的防護包括端點偵測和回應、應用程式隔離和控制、

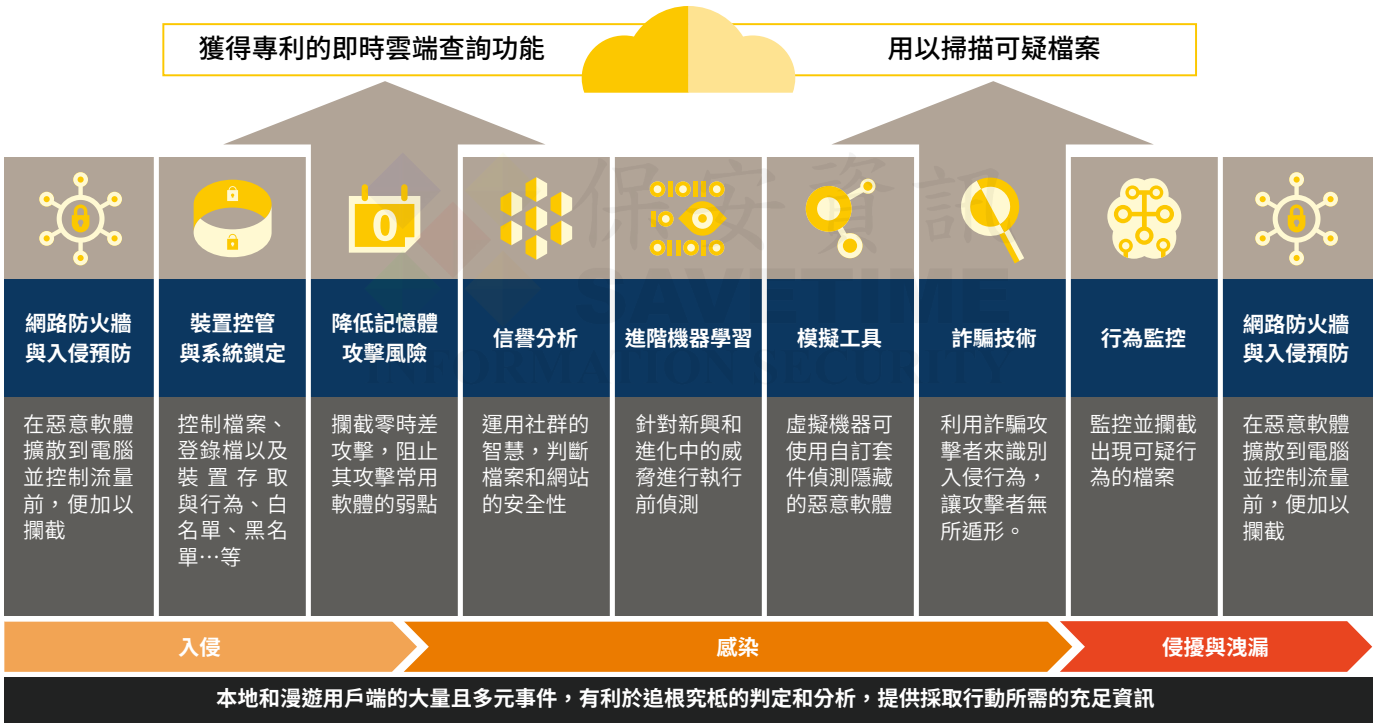

圖 1：業界最深層的偵測技術組合--借助鉅細靡遺的多層次防護來阻擋目標攻擊和零日威脅

對 ActiveDirectory 的保護等。賽門鐵克致力於其自有產品的功能整合，其產品組合以及更大範圍的目標安全和管理生態系統，這就是為什麼賽門鐵克 Endpoint Security 能夠提供如此完整的解決方案。沒有其他供應商可以匹敵 Symantec 的整合，因為它能夠簡化操作並減少“接縫”以保護端點免受各面向的攻擊。

賽門鐵克與產品的整合

使用單一代理程式架構，提供了真正的整合和協調功能，從 Symantec Endpoint Security 的核心防護功能開始，並增加了偵測和回應、誘捕欺騙和強化功能。所有不同功能（單一代理程式，單一主控台）能協同工作，並盡可能以最有效的方式自動識別、處理和解決安全問題。

例如，當在端點上啟動新執行緒時，會自動檢查其信譽。如果該執行緒為已知的善意程式或惡意軟體，則將分別允許或阻止它。如果其信譽未知，則可以根據其屬性將其放入高、中或低安全性沙箱中偵測。這為你提供了一種執行後保護方法，該方法允許用戶可以不受干擾地常態工作，同時減輕了“灰色”應用程式帶來的任何風險。

如果 Symantec Endpoint Security 的行為分析引擎識別出可疑的 PowerShell 命令，則會將其發送給其他引擎進行分析。它還可以使用沙箱進行引爆和深度分析。關鍵是各種防護引擎會協同工作，直到可以確定該活動是惡意的還是善意的。

賽門鐵克的進階機器學習 (AML) 演算法在某種程度上使整合成為可能，該演算法使安全引擎可以從過去的事件中學習，並將這些學習結果自動納入未來的分析和行動中。賽門鐵克不斷地重新審視其工作，並持續地對其演算法進行再訓練，以產生更新更好的分類引擎，從而可以更準確地識別和應對威脅的出現。這是 Symantec 獨有的優勢，主要是因為此類深度分析需要海量資料，只有 Symantec 全球情報網路 (GIN) 才能提供。GIN 收集來全球 1.75 億個端點，8000 萬個 Web 代理程式用戶和 6300 萬個電子郵件用戶的遠端監控，每天產生超過 80 億個信譽請求，每年產生 20 兆次安全事件。[7]

[7] “Machine Learning: Symantec’s Past, Present, and Future,” by Joshua Abramson, Symantec, June 27, 2018, https://www.symantec.com/blogs/feature-stories/machine- learning-symantecs-past-present-and-future.

Symantec AML 可以使用所有這些資料來同時執行數千個檢查。它會自動合併數兆個安全事件以關聯各個接觸點，找到最有可能的路徑，然後構建整個攻擊鏈，以準確了解正在發生的事情（賽門鐵克稱之為“爬行”）。這樣，賽門鐵克就可以即時了解那些事件正在發生，判別出那些事件是惡意或善意，並將這些情資回報到 Symantec 使用的自動化分析和回應解決方案中。

賽門鐵克與產品組合的整合

賽門鐵克端點安全可以輕鬆與其他賽門鐵克解決方案整合，以擴展其功能和價值。該整合解決方案看起來和操作就像單一解決方案，並具有一個可用於監視和管理所有內容的管理主控台。參見圖 2。

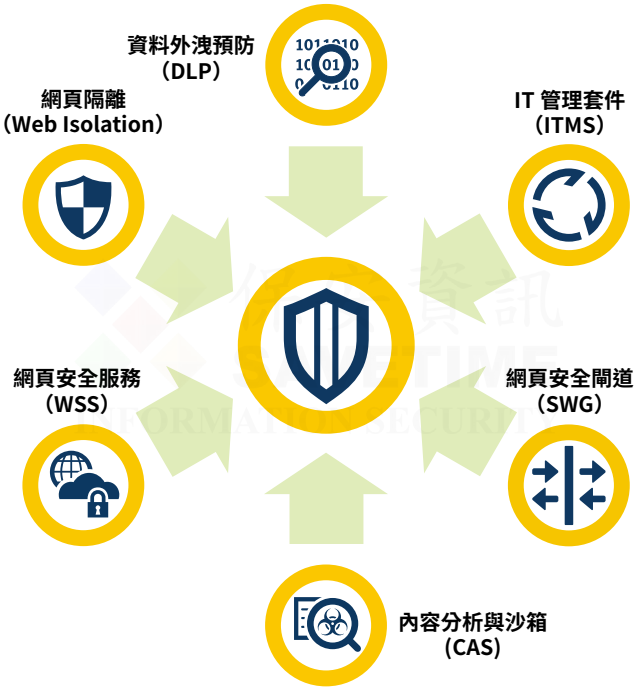

圖 2：只有賽門鐵克端點安全解決方案，才能同時整合所有的功能

- **賽門鐵克資料防洩漏防護 (DLP)** 可發現，監視和保護可疑過程中的機密內容，以支援你的安全性和合規性計劃。例如，Endpoint Security 能阻止可疑執行緒存取由 Data Loss Prevention 歸類為機密的受控管檔案。
- **Symantec Web Isolation** 適用於整合 Web 和端點隔離。Web Isolation 可以自動隔離雲端中的可疑網頁，若於端點上發現的可疑內容則可以使用 Endpoint Security 的應用程式強化功能隔離，這些都可幫助保護你的組織免受惡意軟體和網路釣魚威脅的侵害。

- **Symantec Web Security Services(WSS)** 為遠端存取客戶端提供 Web 防護政策和惡意軟體威脅解決方案。由 Symantec Endpoint Security 可設定將所有 Web 流量強制路由到 WSS 雲端代理程式，這樣漫遊端點就可以實現額外的網路保護。無論用戶是在遠端還是在企業防火牆之後，都可以在整個環境中實施一致的 Web 政策，並使你能夠輕鬆地偵測、識別、阻止和矯正裝置上的威脅和其他安全風險，見圖 3。

圖 3：端點安全--與網頁安全服務 (WSS) 整合

❶ 管理員使用 Web 安全服務主控台建立自定義的 PAC 檔案（可提供自定義略過特定服務器的功能），並將其與明確的代理程式位置相關聯。

❷ 管理員存取端點管理主控台並設定 Web 流量重導向 (WTR)，其中包含了建立的 PAC 檔案。

❸ 端點管理主控台將安全政策（包括 PAC 檔案 URL）分派到端點。代理程式接收安全政策後就會為系統和瀏覽器配置代理程式設置。

❹ PAC 檔案將所有 Internet 流量轉導向到代理程式最近的 Web 雲端安全服務，以進行 Web 使用和安全政策處理。

- **Symantec Content Analysis(CA)** 可驗證和加強入侵偵測。可疑或惡意檔案將會送到 CA（或第三方引擎）以進行沙箱分析。一旦被識別為惡意檔案，你可以快速將其加到 Endpoint Security 的黑名單中，這樣其他任何終端用戶都無法再執行該檔案，且阻止其在網路上傳播。此外，管理員可以讓 Endpoint Security 運行矯正政策以清理端點上的原始感染。

- **Symantec Secure Web Gateway(SWG)** 支援網路層級上的端點偵測和修復。例如，當 SWG 偵測到檔案為惡意檔案時，它可以查詢 Endpoint Security 以確定有多少個裝置擁有相同的檔案，然後觸發 Endpoint Security 來阻止或刪除這些檔案。

- **賽門鐵克 IT 管理套件 (ITMS)** 可簡化修正檔程式管理，並輕鬆關閉“接縫”並使端點保持最新狀態。ITMS 可以與 Endpoint Security 進行協調，以針對 Windows 或其他第三方應用程式，若沒安裝關鍵安全修正檔的端點將其自動隔離，直到該端點安裝了修正檔才會將其釋出。

賽門鐵克與生態系統的整合

賽門鐵克能讓所有供應商或內部開發人員都可以使用開放的 API 存取所有內容，以擴展和增強 Symantec 解決方案的功能。參見下面的圖 4。

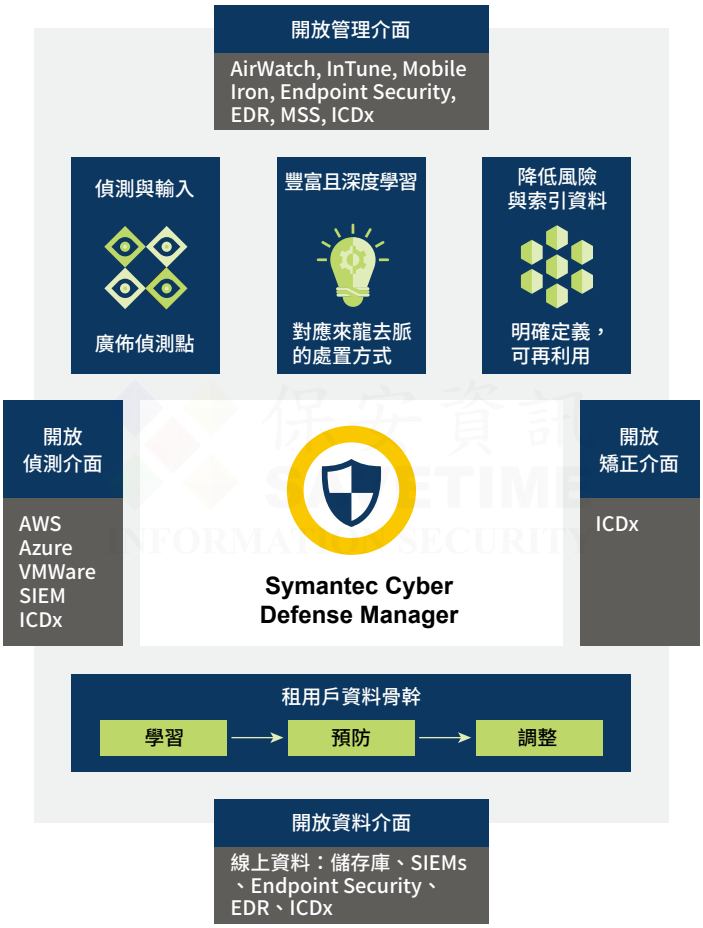

圖 4：Symantec Cyber Defense Manager 開放、聰明的雲端主控台，管理完整的端點安全，降低安全管理複雜度

賽門鐵克已採用 OpenC2[8] 語言進行機器對機器的通信，這是 API 存取的行業標準。這樣可以對威脅進行自動化、協調性、戰術性的回應，從而幫助你的組織“以網路速度緩解攻擊”。

賽門鐵克的開放框架允許輕鬆地輸出資料，以改善威脅情報和其他解決方案的回應。它還可以允許上傳資料，以增強 Symantec 在環境中識別和回應事件的能力。

例如，你可以使用 SIEM 提供的 syslog 或連接器整合安全事件和事件管理 (SIEM) 系統，以加強 Endpoint Security 與其他第三方安全產品和威脅情報資料源的事件關聯。

你還可以整合網路存取控制 (NAC) 產品 (例如：ForeScout)，以防止被感染或被入侵的端點連接到公司網路。Endpoint Security 擴展模組使用 ForeScout 的 CounterACT 來驗證代理程式的完整性，觸發即時惡意軟體掃描並幫助在裝置連接時強制合規。它還提供自動回應選項，以隔離或限制不合規或受感染裝置的網路存取，並促進補救措施。因此，你可以減少被攻擊面，最大程度地減少惡意軟體的傳播，並降低資料洩露的影響[9]。

這只是 Symantec 與整個端點管理和安全生態系統中的供應商整合的例子之一 (可於如下連結此處找到許多其他整合方案：https://broadcom.com/products/cyber-security)。

使用 Symantec，你可以靈活地自行決定要部署何種安全功能，以滿足你的獨特需求。你可以自定政策和工作流程，以進一步簡化和優化端點安全強制性。例如，你可以通過 API 自動將端點移動到管理主控台中的其他群組。通過使用 REST API，可以輕鬆地促進與這些類型的自定義腳本或其他產品的整合。

結語

端點環境充滿了複雜性，這對安全性不利。市面上有很多種解決方案可幫助你獲得控制權並消除任何“接縫”，但很不幸往往最終會加劇該問題嚴重性。我們需要一種整合的端點管理和安全性方法，該方法要能有效保護你的資料和資源免受端點攻擊，同時簡化操作並降低總擁有成本。

Symantec Endpoint Security 就是能達到此要求的產品，它通過單一代理程式架構以行業領先的效率，保護你的端點免受所有攻擊媒介的侵害。Endpoint Security 通過協同運作的威脅偵測和回應，誘捕欺騙和強化功能奠定了基礎，使你可以通過單一代理程式，單一主控台查看和控制端點環境。Endpoint Security 通過開放的 API 能與自有的 Symantec 解決方案或第三方產品完美整合，以確保你具有建立和維護法規遵從性所需的全部功能以及強大的安全性。

賽門鐵克的整合方法擁有獨一無二的大量威脅情報，結合了雲端和本地端安全性，以保護用戶、資料、訊息和網路。賽門鐵克的整合解決方案共享情報，並且可以一起保護你的網路--沒有其他供應商能提供類似的統合解決方案，此解決方案可以協調跨 Web、電子郵件、雲端和閘道的威脅情資，進而觸發端點正確回應。通過 Symantec 產品、產品組合和生態系統的整合，你可以大大簡化端點安全性，故可以從安全性投資中獲得更好的總體防護和更大的總體價值。

更多訊息

更多有關詳細情報，請存取 Symantec Endpoint Security 網站 https://www.broadcom.com/products/cyber-security/endpoint/end-user。

[8] OASIS Open Command and Control (OpenC2) TC, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2, https://www.youtube.com/watch?v=kCooyNJoOrU.

[9] “ForeScout Extended Module for Symantec Endpoint Protection,” https://www.forescout.com/wp-content/uploads/2017/03/ForeScout-Extended-Module-for-Symantec-Endpoint-Protection-Datasheet.pdf.

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策略性整合式解決方案，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

Copyright ©2019 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

20B283330_WP_Value_of_Integration_Endpoint_EN