解決方案簡介

Symantec Endpoint Protection 14.3 RU9

專為雲端世代打造，最完整的端點安全解決方案

快速一覽

運用單一代理程式基礎架構，以領先業界的優異成效保護端點，並抵禦所有攻擊媒介的威脅

- 賽門鐵克端點防護 (SEP14.3 RU4 開始) 針對加密勒索軟體最棘手的就地取材攻擊的強化防護技術說明
- 最新版--賽門鐵克端點防護 (SEP14.3 RU9) --新增功能說明。
- 多層式防護解決方案結合了進階機器學習、行為分析及刺探預防等非病毒特徵性技術，以及入侵預防、信譽分析等經過驗證的保護功能，能夠抵禦勒索軟體和其他新興威脅
- 透過調適防護功能，提高對可疑檔案的能見度，以便做出更為妥善的政策決定
- 使用欺敵技術來揭露隱藏的攻擊者，判斷他們的攻擊意圖，進而改善安全態勢
- 保護常用的應用程式，杜絕漏洞刺探攻擊，並從惡意活動隔離可疑的應用程式

大規模實現整合式網路防禦

- 運用 SEP 並整合網頁和電子郵件閘道等網路安全基礎架構，在任何地點偵測威脅並加以應變
- 運用相同的 SEP 代理程式，並整合 Endpoint Detection and Response (EDR)，以執行資安事端調查和回應
- 整合現有 IT 基礎架構，以便運用開放 API 進行自動化和協調

使用高效能、輕量化的解決方案推動業務

- 運用網路頻寬限制最佳化端點內容更新頻率，且不會犧牲安全成效
- 藉由頻寬用量最少的輕量化代理程式和病毒定義組，大幅提升效能 (比 SEP12 少 70%)
- 藉由提升掃描速度的進階設計技術和獲得專利的即時雲端查詢，加速偵測 (比 SEP12 快 15%)

簡介

隨著今日的 IT 環境持續演變，攻擊者正使用更加複雜的攻擊手段來滲透到網路中，而端點便成為了最後一道防線。隨著勒索軟體攻擊日益盛行，而此現象從 WannaCry 和 Petya 的爆發便可見一斑，這也讓企業愈來愈擔憂類似攻擊所帶來的網路危害和營運中斷的情況。此外，攻擊者廣泛使用無檔案式的隱匿攻擊，結合「自給自足」戰術 (即利用常見 IT 工具進行攻擊)，進一步危及端點資產的機密性、完整性和可用性。

那麼安全團隊該怎麼做才能抵禦網路攻擊？管理多個端點產品和技術無疑是一項艱難挑戰，而若要涵蓋多個地點，針對多種作業系統和平台的安全性作業進行管理，困難程度還會加倍。僅擁有有限資源和預算，安全團隊需要易於管理的技術，以便進行相互整合，進而提升整體安全性。他們不需要「另一款端點產品」。請參閱圖 1。

Symantec Endpoint Protection (SEP) 可提供優異的多層式防護功能，無論端點遭到何種形式的攻擊，都能夠阻擋威脅。SEP 與現有安全基礎架構進行整合，能提供協調式回應，迅速解決威脅。單一輕量化 SEP 代理程式提供高效能，同時又可兼顧一般使用者生產力，因此您可以專注於您的業務。如圖 2 的安全性架構所示，SEP 可以讓資安人員在許多安全性使用案例上執行作業。

圖 1

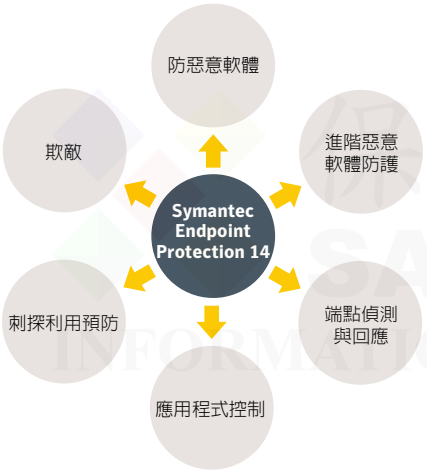


圖 2：SEP 安全性架構

運用單一代理程式基礎架構，以領先業界的優異成效保護端點，並抵禦所有攻擊媒介的威脅

預防

如圖 3 所示，無論攻擊者從攻擊鏈的哪個位置襲擊，SEP 都可以保護端點。SEP 領先業界的安全性成效經過第三方驗證。結合核心技術以及新穎頂尖的技術，才能實現如此高等級的防護效果。

圖 3

非病毒特徵型技術

- **進階機器語言 (AML)**--偵測全新以及演進中的威脅，預先執行。
- **降低記憶體攻擊風險**--可針對常見軟體的漏洞，攔截並阻止零時差攻擊。
- **行為監控**--監控並攔截出現可疑行為的檔案。

進階功能

- **全球智慧型網路 (GIN)**--藉由在 157 個國家中的 1.75 億個端點及 5,700 萬個攻擊偵測器，提供全球規模最大的民間威脅情報網路。所收集的資料由超過一千名高技能威脅研究人員進行分析，針對威脅提供獨特能見度，並開發先進的安全創新功能。
- **信譽分析**--使用位在雲端並有 GIN 提供支援的人工智慧技術，判別檔案和網站的安全性。
- **模擬器**--使用精簡版沙箱，來偵測經自訂套件隱藏的變種惡意軟體。
- **智慧型威脅雲端**的快速掃描功能，使用流水線操作、信任散播以及批次查詢等進階技術，因此無須將所有特徵定義檔案下載到端點，進而維持高效率作業。因此，它只會下載最新的威脅資訊，使病毒特徵定義檔案的大小減少 70%，連帶也能減少頻寬使用量。
- **Secure Web Gateway 整合性**--全新可編程的 REST API，實現和 Secure Web Gateway 等現有安全基礎架構整合的可能性，進而在端點協調回應，快速終止感染擴散。

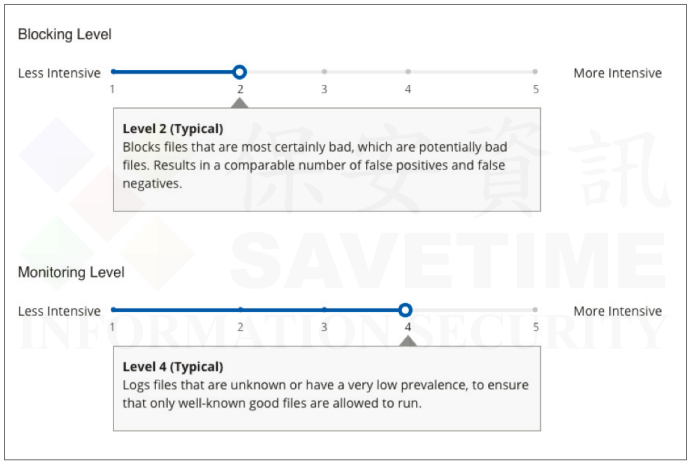
核心功能

- **防毒**--在惡意軟體感染系統之前，加以掃描並且根除。
- **防火牆和入侵預防**--在惡意軟體擴散至機器前加以攔截，並控制流量。
- **應用程式與裝置控制**--控管檔案、系統登錄、裝置存取和行為，以及提供白名單與黑名單。
- **Power Eraser**--能遠端觸發的強力工具，可以解決進階持續性威脅，並清除頑強的惡意軟體。
- **主機完整性**--確保端點受到完善保護並且符合強制執行的政策，偵測未經過授權的變更，執行損害評估，並能隔離沒有滿足要求的受管理系統。
- **系統鎖定**--允許白名單應用程式 (善意) 得以執行，並阻擋黑名單應用程式 (惡意) 之執行。

此外，如圖 4 所示，SEP 可以讓 IT 安全團隊調適偵測和攔截等級，進而最佳化防護功能，並且為每名客戶提升可疑檔案的能見度。這個可調適的安全功能稱為密集型防護，採用全新的雲端主控台，並自動整合了內部部署的 SEP Manager，能夠輕易針對可疑檔案或任何誤報進行黑名單或白名單操作。

賽門鐵克的單一代理程式基礎架構，能讓 IT 安全團隊以簡化部署方式新增創新的安全性技術，也就是不需要新的代理程式。

圖 4：透過密集型防護進行可調適監控和攔截



偵測與回應 (EDR)

Symantec Advanced Threat Protection：運用 SEP 中的整合式 EDR 功能，為端點提供資安事端調查和回應。部署可在一小時內完成，透過精準的機器學習、行為分析和減少誤報的威脅情報來揭露進階攻擊，協助確保安全團隊的高生產力。賽門鐵克的 EDR 功能讓資安事端應變人員快速搜尋、辨識和控制所有受到影響的端點，同時使用內部部署沙箱和雲端沙箱來調查威脅。此外，持續記錄系統活動，支援全面的端點能見度和即時查詢。

Symantec ENDPOINT DETECTION AND RESPONSE (EDR):

- **偵測和揭露**--減少漏洞搜尋所需時間，並快速揭露影響範圍。
- **調查和控制**--提高資安事端應變人員的生產力，確保威脅控管能力。
- **解決**--快速修正端點，確保威脅不會再次出現。
- **提高安全性投資效益**--預先建立的整合功能和公用 API。

欺敵

SEP Deception[1] 會部署欺敵戰術（即誘餌）並透過早期能見度來揭露隱藏的攻擊者及其意圖和戰術，並運用此資訊來提升安全態勢。SEP Deception 擁有準確且富含洞察力的偵測功能，同時能快速實現資安價值。Symantec Endpoint Protection 和賽門鐵克安全委外管理服務的共同客戶，將能受益於由全球專家團隊提供的全天候即時 SEP Deception 監控和回應服務。賽門鐵克是唯一一個提供 Deception 功能的端點防護平台供應商。

SEP Deception：

- 使用誘騙和誘餌的主動式安全功能，能夠揭露並延誤攻擊者的行為。
- 判定攻擊者意圖，進而改善安全態勢。
- 提供大規模誘餌手段，簡化部署和管理。

調適

SEP 強化是以雲端提供的進階應用程式防禦解決方案，透過隔離可疑應用程式，並保護受信任的應用程式，來提供完整的應用程式防護功能。和其他應用程式隔離供應商提供的端點產品不同，SEP Hardening 結合 SEP，針對惡意軟體和可疑應用程式提供空前成效。此外，由於 SEP Hardening 完整支援標準員工工作流程，能夠維持員工的高生產力。

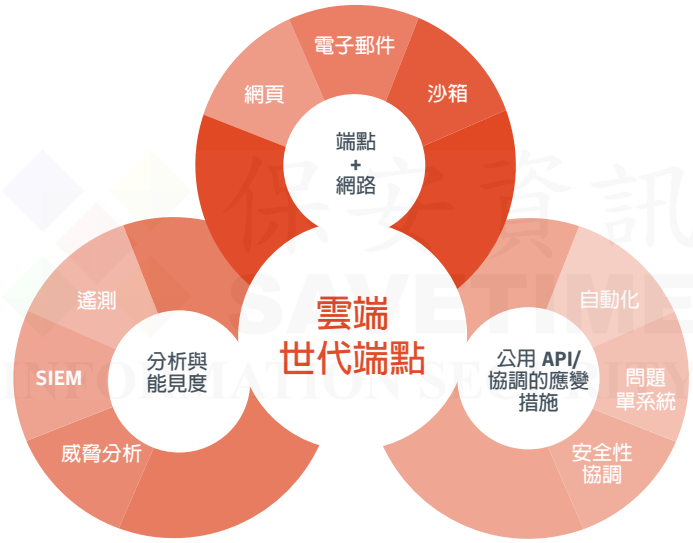
SEP Hardening：

- 減少攻擊介面，提供完整全面的應用程式安全性。
- 搜尋並分類所有端點應用程式，提供空前能見度。
- 利用 SEP 的單一代理程式基礎架構，能以最快速度帶來資安投資價值。

[1] 需要顧問服務來設定和部署 SEP Deception 功能。

圖 5：SEP Deception 如何運作？

圖 6



大規模實現整合式網路防禦

大多數大型企業支援日益複雜的全球 IT 環境，但他們實施的許多解決方案卻只能進行某項特定工作。因此，企業需要一款能夠提供更多價值的解決方案，並能整合其他 IT 安全解決方案，透過共享情報並一同進行網路防護作業，帶來更為全面的防護效果。

SEP 14 是一款基礎產品，可加快功能整合，並讓 IT 安全團隊，在任何地點偵測網路中的威脅，並透過協調回應來加以解決。SEP 14 能夠和賽門鐵克解決方案 (例如做為整合式網路防禦平台的主要元件) 或第三方產品 (透過公用 API) 搭配使用，進而提升安全態勢。賽門鐵克整合式網路防禦平台結合雲端和內部部署的安全功能，可以保護使用者、資訊、即時訊息和網路，並由無與倫比的威脅情報提供強大支援。賽門鐵克是唯一一家提供整合式解決方案的供應商，能夠在網路閘道 (網頁和電子郵件安全閘道) 進行威脅偵測，並觸發端點協調回應 (黑名單和矯正)。

使用高效能、輕量化的解決方案推動業務

大型及／或頻繁的內容更新占用頻寬，降低端點效能和生產力。最佳化內容更新並提供更為出色的威脅偵測，無疑是雙贏局面。這些功能可以減少 IT 團隊頻繁安排安全性更新時的繁重負擔。一般使用者則不會因為安全性更新而影響生 產力。

SEP 14 提供更為出色的防護功能及效能，卻僅需要較少頻寬需求。賽門鐵克持續在第三方效能測試中最高分數成績，包括 Passmark Software Windows 7 和 Windows 10 企業端點安全效能標竿測試。造訪賽門鐵克效能中心，瞭解額外的第三方驗證資訊 https://www.broadcom.com/solutions/integrated-cyber-defense。

SEP 重大效能改善包括：

- 減少內容更新大小達 70%[2]
- 提高更快速的偵測掃描時效，高達 15%[2]

和新興的供應商相比，SEP 在單一輕量化代理程式中整合多個功能，進而降低端點複雜度。若要試圖達到與賽門鐵克的端點安全功能匹敵，將需要多個新興供應商、多款解決方案，當然也需要多個代理程式。

[2] 從 SEP 12 升級至 SEP 14 的效能提升。

系統需求 ～ 14.3、最新版14.3RU9

SEP用戶端系統需求(桌機、筆電、工作站以及伺服器)

Windows® 作業系統

作業系統 (桌面)

如需目前版本和舊版支援的作業系統清單，請參閱：

Windows 與 Endpoint Protection 用戶端的相容性

- 從 14.3 RU8 開始，您必須在用戶端上安裝 Microsoft Azure Code Signing (ACS) 支援。Microsoft ACS 支援僅適用於 Windows 8.1 和更新版本。

  以 Microsoft Azure Code Signing (ACS) 支援升級 Windows 用戶端電腦 14.3 RU8 及更新版本

- 14.3 RU6 和更新版本不再支援執行 Microsoft Windows 32 位元作業系統的電腦。32 位元的電腦應執行 14.3 RU5 客戶端。

作業系統(伺服器)

如需目前版本和舊版支援的作業系統清單，請參閱：

Windows 與 Endpoint Protection 用戶端的相容性

如要在 Windows 7、Windows Server 2008 或 Windows Server 2008 R2 上接收最新的 SONAR、CIDS 或 ERASER 內容，請參閱：

Windows 7、Windows Server 2008 和 2008 R2 的 SONAR 12.3.0、CIDS 17.2.6 和 ERASER 119.1.3 作業系統需求

Windows 硬體需求

- 2 GHz CPU 或更快的處理器
- 1 GB 記憶體 (建議使用 2 GB)或更多 (如果作業系統需要)
- 545 MB 可用硬碟空間(暗網)

Macintosh® 作業系統

- macOS 10.15 到 10.15.7
- macOS 11.x (Big Sur)
- macOS 12.x (Monterey)(自SEP 14.3 RU3起)
- macOS 13 (Ventura)
- macOS 14 (Sonoma)

如需以前版本受支援的作業系統清單，請參閱：Mac 與 Endpoint Protection 用戶端的相容性

虛擬環境

- Microsoft Azure
- Amazon Web Service (AWS) EC2
- Amazon 工作區
- Citrix Studio 2009.0.0 版
- Nutanix AOS 5.15 (LTS)
- Oracle Cloud Infrastructure (OCI)
- VMware WS 5.0 (工作站) 或更新版本
- VMware GSX 3.2 (企業) 或更新版本
- VMware ESX 2.5 (工作站) 或更新版本
- VMware ESXi 4.1 至 6.0 Update 2
- VMware ESXi 6.0 Update 3 (自 14.0.1 起)
- VMware ESXi 6.5 (自 14.0.1 起)
- VMware ESXi 6.5U1 (自 14.2 起)
- VMware ESXi 6.5U2 (自 14.2 起)
- VMware ESXi 6.7 (自 14.2 起)
- VMware ESXi 7.0 Update 2 (自 14.3 RU2 起)
- Microsoft Virtual Server 2005
- Windows Server 2008 Hyper-V
- Windows Server 2008 R2 Hyper-V
- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V
- Windows Server 2016 Hyper-V (自 14.2 MP1 起)
- Windows Server 2019 Hyper-V Core Edition (自 14.2 MP1 起)
- Citrix XenServer 5.6 或更新版本
- Virtual Box (由 Oracle 提供)

※更詳細資訊請參考：
最新支援的虛擬環境

Linux 作業系統 (32 位元和 64 位元版本)

- Amazon Linux和Linux 2
- CentOS 6U3 - 6U9, 7 - 7U7, 8; 32 位元和 64 位元
- Debian 6.0.5 Squeeze, Debian 8 Jessie; 32 位元和 64 位元
- Fedora 16, 17; 32 位元和 64 位元
- Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4
- Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U7, 8-8U2
- SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32 位元和 64 位元; 12, 12 SP1 - 12 SP3, 64 位元
- SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32 位元和 64 位元; 12 SP3, 64 位元
- Ubuntu 12.04, 14.04, 16.04, 18.04(截至 14.3); 32 位元和 64 位元

自版本 14.3 RU1 起支援的作業系統：

- Amazon Linux 2023
- Amazon Linux 2
- CentOS Linux 7, 8*
  自 SEP 14.3 RU9 起不支援 CentOS Stream
- Debian 10 (14.3 RU2 和更新版本)
- Oracle Enterprise Linux 6、7、8
- Rocky Linux 8、9
- Red Hat Enterprise Linux 6、7、8、9
- SuSE Linux Enterprise Server 12.x、15.x
- Ubuntu 16.04 LTS、18.04 LTS、20.04 LTS、22.04 LTS(14.3 RU6 和更新版本)

※更詳細資訊請參考：
SEP 14.3 RU8 最新 Linux 支援

Linux 硬體需求

- 具 4 個以上核心的 Intel Xeon 或更快的處理器
- 至少 512 MB 的可用 RAM (建議使用 4 GB)
- 7 GB可用硬碟空間(如果 /var、/opt 和 /tmp共用相同的檔案系統/磁碟區，則有2 GB可用磁碟空間；如果是不同的磁碟區，則每個 /var、/opt 和 /tmp 中有 1 GB 可用磁碟空間)
- 若啟用任何 Symantec Endpoint Detection and Response 功能，建議在 /opt 中額外增加 5 GB 磁碟空間。

Mac 硬體需求

- 64 位元 Intel Core 2 Duo 或更新版本的處理器
- Apple M1 晶片(自SEP 14.3 RU2起)
- 2 GB 記憶體/1 GB 可用硬碟空間
- Apple M2 晶片 (自 14.3 RU5 起)

Manager系統需求

Windows® 作業系統

- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022(自14.3 RU3起)

網頁瀏覽器

- Microsoft Edge Chromium 型瀏覽器 (SEP 14.3 及更新版本)
- Microsoft Edge
  注意：32 位元版本的 Windows 10 不支援在 Edge 瀏覽器上存取 Web 主控台
- Microsoft Internet Explorer 11 (SEP 14.2.x 及更舊版本)
- Mozilla Firefox 5.x 至 107
- Google Chrome 113 至 115

硬體

- 最低需求為 Intel Pentium 8 核心或同等級的處理器
- 2 GB 記憶體 (建議使用 8 GB或更多可用空間)
- 硬碟空間：最小需40GB(使用內嵌資料庫或本機SQL資料庫，建議200GB、使用遠端SQL資料庫，建議100GB)

資料庫

Symantec Endpoint Protection Manager 包括一個預設資料庫：

- Microsoft SQL Server Express 2014 (適用於 Windows Server 2008 R2)
- Microsoft SQL Server Express 2017
- Sybase 內嵌資料庫 (僅 14.3 MP.x 和更舊版本)，如有升級至14.3RU1及更新版本，歡迎洽詢保安資訊，因新版本內嵌資料庫已改採MS-SQL express，我們的實務經驗可以協助您，減少嘗試錯誤，更輕鬆簡單轉移至新版本。

您也可以選擇使用下列其中一種 Microsoft SQL Server 版本的資料庫：

- SQL Server 2012 RTM-SP4(14.3 RU5 及更早版本)
- SQL Server 2014 RTM - SP3
- SQL Server 2016 SP1、SP2
- SQL Server 2017 RTM
- SQL Server 2019 RTM (14.3 及更新版本)
- SQL Server 2022 (14.3 RU6 及更新版本)

*欲取得系統需求的完整清單，請造訪支援頁面

關於賽門鐵克端點防護

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。

若想瞭解更多本解決方案資訊，請造訪保安專屬網頁 **http://www.savetime.com.tw/symantec/sep.asp**

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