Symantec ™ Endpoint Protection 14

產品型錄：端點安全

概述

去年，我們共發現 4.31 億支全新的惡意程式變種，注意到勒索軟體的攻擊形態越來越詭譎多變，零時差威脅的數目也足足成長了兩倍。[1] 隨著威脅環境迅速演變，在現今網路的規模和複雜性之下，企業要迎頭趕上十分困難。許多廠商和新創公司試著採用其他方法和單一功能解決方案，來遏止惡意程式的感染，但防護成效卻很有限。相信所有人都認同，端點安全極為重要，但要提供一套有效的解決方案，卻變得比以往都來得困難。

為了防禦現今複雜的威脅態勢，無論企業端點遭受何種形態的攻擊，客戶都必須設法遏止這些威脅。要達成這項目標，企業需要具備這些特定的功能：

- 可偵測未知威脅和預防零時差攻擊 (包括勒索軟體) 的進階技術
- 記憶體攻擊防護能力，以保護常用的應用程式和作業系統免受威脅
- 存取最豐富的全球威脅情報，以即時阻擋威脅
- 協調應變動作，以便迅速阻止威脅
- 在所有裝置提供通過考驗的防護能力，同時兼顧效能

Symantec Endpoint Protection 14 是專門為了解決今日的威脅態勢所設計的產品，可利用全方位的方式，延伸至攻擊鏈並提供更深入的保護。在全球最大民間威脅情報網路的支援下，Symantec Endpoint Protection 14 可透過多面向機器學習、信譽分析與即時行為監控等新一代技術，有效阻止進階威脅。除了必要的預防技術之外，企業的整體防護也一樣重要。Symantec Endpoint Protection 14 可透過單一管理主控台與輕量型代理程式，與安全基礎架構中的其他產品整合，迅速對威脅做出回應，在所有同級產品中提供最佳的端點防護能力[2]，同時兼顧效能。

涵蓋整個攻擊鏈的全方位防護

結合新一代與關鍵技術，無論進階威脅和快速變種的惡意程式如何攻擊端點，都能以高效能的輕量型代理程式加以阻止。

入侵：

- **網路入侵預防、URL 及防火牆政策：**賽門鐵克的網路威脅防護技術可分析入埠和離埠資料，在威脅通過網路入侵端點前加以攔截，同時也提供了規則式防火牆和瀏覽器防護功能，以抵禦網頁式攻擊。整體來說，有如此強大的網路防護，就能在威脅入侵端點前偵測到半數以上的威脅。
- **應用程式行為控管：**控管檔案、系統登錄的存取以及處理程序可執行的方式。
- **裝置控管：**限制特定硬體的存取權限，並控制哪些類型的裝置可上傳或下載資訊。亦可將外部媒體控管與應用程式控管結合，以提供更具彈性的控管政策。

[1] 2016 年賽門鐵克網路安全威脅研究報告
[2] 榮獲 AV-TEST.Org 的 2016 年最佳防護獎

- **攻擊預防：**使 Heap Spray、SEHOP 覆寫和 Java 攻擊等零時差攻擊失去效力，以保護廠商尚未發佈修補程式的常用軟體，避免威脅。無論任何瑕疵、程式錯誤或漏洞，這項非病毒特徵型技術都能發揮效用。

威染：

- **攻擊預防：**在偵測惡意程式預防感染方面，也有出色表現。
- **信譽分析：**賽門鐵克獨特的信譽分析會使用情報網路交叉比對上百億的使用者、檔案與網站間的關聯性，可主動攔截更多威脅，抵禦快速變種的惡意程式。透過分析幾項關鍵檔案屬性，例如檔案的下載次數、存在時間及下載來源，我們就能準確地偵測檔案的好壞，並在檔案到達端點前為每個檔案指定信譽評等。還可根據檔案信譽僅掃描有風險的檔案，有效地大幅減輕掃描負荷。
- **機器學習：**端點上的多面向機器學習可防止新型和未知的威脅，減少對病毒特徵的依賴。使用全球情報網上數以兆計的好壞檔案樣本來訓練機器學習，以大幅降低誤報率。
- **模擬：**高速模擬工具可透過變種的自訂套件，偵測隱藏的惡意程式。靜態資料掃描程式會在輕量型虛擬機器上，以毫秒的速度掃描每個檔案，使威脅無所遁形，同時協助改善偵測率和效能。
- **防毒檔案防護：**特徵式防毒和進階檔案啟發式技術會尋找並根除系統中的惡意程式，藉此抵禦病毒、病蟲、木馬程式、間諜程式、Bot 傀儡程式、廣告軟體和 rootkits
- **行為監控：**雖然有極少數威脅在現階段仍無法偵測，Symantec Endpoint Protection 的行為監控還是非常有效。此技術運用機器學習來提供零時差的防護，可在程式執行時，即時監控將近 1,400 種檔案行為並判斷檔案風險，有效地防止新型和未知的威脅。

侵擾與洩漏：

- **行為監控：**行為監控對於防止感染擴散亦大有助益。
- **網路入侵預防、URL 及防火牆政策：**可分析內傳和外送的資料，在威脅於網路中傳送時加以攔截。

全球威脅情報：我們的新一代技術充分利用獲得專利的即時雲端查詢技巧，可快速存取全球規模最大的民間威脅情報網路。這可提供最新威脅技術的深入資訊強化我們的機器學習功能，為所有端點提供最高等級的防護，並使用雲端演算法以近乎即時的方式更新。從 157 個國家、1.75 億個端點及 5,700 萬個攻擊偵測器收集而來的資料，會由上千位技術高超的威脅研究人員進行分析，以提供獨特的掌握資訊、開發先進的資安創新技術，藉此對抗威脅。

提供高效能的進階功能

Symantec Endpoint Protection 不僅涵蓋了各式各樣的技術，更經過最佳化，能夠讓網路或使用速度都不受影響。就效能而言，我們亦持續在各項第三方測試中保持領先。

- 智慧型威脅雲端的快速掃描功能，使用多項先進技術 (例如pipelining、信任推演與批次詢問)，因此不須將所有病毒特徵定義檔下載至端點，即可維持高水準的成效。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。
- 透過端點進階機器學習所提供的額外成效，不僅可減少下載頻率，由於誤報使作業中斷而影響生產力的情況也會大幅減少。
- 這個單一輕量型代理程式，具備了通常須透過多個代理程式才能取得的技術和功能，包括：機器學習、攻擊緩和、端點偵測和回應 (EDR) 以及防惡意程式功能。這代表企業將得以減少他們必須在端點上管理的代理程式數量，進而提升效能，同時減輕 IT 人員的負擔以及並降低整體持有成本。

在端點上輕鬆整合，以便採取妥善協調的應變動作

Symantec Endpoint Protection 包含一個主控台與代理程式，可為各個作業系統、平台和任何規模的企業提供保護。

- **Power Eraser：**這款主動式工具可從遠端觸發，以找出進階持續性威脅，並矯正頑強的惡意軟體。
- **主機完整性檢查：**藉由強制執行政策、偵測未經授權的變更並執行損害評估，以及找出不符合您需求的受管理系統，以確保端點受到保護並遵循法規。搭配使用威脅偵測產品，透過妥善協調的應變動作將受感染的端點隔離，在您矯正端點或為其重新建立影像前，迅速阻止感染散佈。
- **系統鎖定：**允許執行許可清單中的應用程式 (已知為善意的程式)，或封鎖執行黑名單上的應用程式 (已知為惡意程式)。Symantec Advanced Threat Protection (ATP) 和 Secure Web Gateway 可透過可程式化的 API 與 SEP 管理 (SEPM) 主控台溝通，並協調適當的應變動作，利用應用程式控管將新發現的惡意應用程式加入黑名單中。可在 Windows®、Mac®、Linux®、虛擬機器和內嵌式系統上執行。

- **Secure Web Gateway 整合性：**新的可程式化 REST API 實現了與第三方產品整合的可能 (包括 Secure Web Gateway)，並可在端點上協調的應變動作，迅速阻止感染散佈。

- **EDR 主控台 (ATP:Endpoint) 整合性：**Symantec Endpoint Protection 已與 Symantec EDR 主控台 (Advanced Threat Protection (ATP:Endpoint)) 整合，可排定攻擊的優先順序，更快速地偵測目標式攻擊和進階持續性威脅，並做出回應且加以封鎖。EDR (端點偵測和回應) 功能已內建於 Symantec Endpoint Protection，因此無需部署額外的代理程式。

保護、效能與回應

Symantec Endpoint Protection 在端點防護領域始終維持領導者地位：

- 屢屢獲得 SE Labs[3] 給予的 AAA 等級評價 (最高評分)。[3]
- 通過 A/V Test[4]，在 18 個月間 100% 抵禦零時差攻擊
- 過去 14 年在 Gartner 神奇象限中始終維持領導者評等[5][5]

[3] SE Labs 的網址為 https://selabs.uk/en/reports/enterprise
[4] AV Test 的網址為 https://www.av-test.org/en/antivirus/business-windows-client/
[5] 2016 年 2 月的 Gartner 神奇象限

用戶端工作站與伺服器系統需求 *	
Windows 作業系統	**虛擬環境**
Windows Vista (32 位元、64 位元)	Microsoft Azure
Windows 7 (32 位元、64 位元、RTM 和 SP1)	Amazon WorkSpaces
Windows 7 Embedded Standard	VMware WS 5.0、GSX 3.2、ESX 2.5 或更新版本
Windows 8 (32 位元、64 位元)	VMware ESXi 4.1 至 5.5
Windows 8 Embedded (32 位元)	VMware ESX 6.0
Windows 8.1	Microsoft Virtual Server 2005
Windows 10	Microsoft Enterprise Desktop Virtualization (MED-V)
Windows Server 2008 (32 位元、64 位元，包括 R2)	Microsoft Windows Server 2008、2012 及 2012 R2 Hyper-V
Windows Essential Business Server 2008 (64 位元)	Citrix XenServer 5.6 或更新版本
Windows Small Business Server 2011 (64 位元)	Oracle 的 Virtual Box
Windows Server 2012 (64 位元，包括 R2)	**Linux 作業系統 (32 位元與 64 位元版本)**
Windows Server 2016	Red Hat Enterprise Linux
Windows 硬體需求	SUSE Linux Enterprise (伺服器 / 桌上型電腦)
1 GHz 或更快的處理器	Oracle Linux (OEL)
512 MB 記憶體 (建議使用 1 GB)	CentOS
1.5 GB 可用硬碟空間	Ubuntu
Macintosh 作業系統	Debian
Mac OS X 10.9、10.10、10.11、Mac OS 10.12	Fedora
Mac 硬體需求	**Linux 硬體需求**
64 位元 Intel Core 2 Duo 或更新的處理器	Intel Pentium 4 (2 GHz CPU 或更快的處理器)
2 GB 記憶體	1 GB 記憶體
500 MB 可用硬碟空間	7 GB 可用硬碟空間

Manager 系統需求	
Windows 作業系統	**硬體**
Windows Server 2008 (64 位元，包括 R2)	最低需求為 Intel Pentium 雙核心或同等級的處理器
Windows Server 2012 (R2)	2 GB 記憶體 (建議使用 8 GB)
Windows Server 2016	8 GB 或更多的可用硬碟空間
Mac 硬體需求	**資料庫**
Microsoft Internet Explorer	內含內嵌資料庫或可選擇下列資料庫：
Mozilla Firefox	SQL Server 2008 R2、SP3、SP4
Google Chrome	SQL Server 2012、RTM - SP1；SP2
Microsoft Edge	SQL Server 2014、RTM 及 SP1
	SQL Server 2016

* 如需完整的系統需求清單，請造訪我們的支援頁面

**Symantec ™ Endpoint Protection 12.1.6 MP1a 新增的支援

請注意：Symantec ™ Endpoint Protection 12.1.6 MP2 支援 Mac OS X10.11

更多資訊

立即免費試用

現在就下載免費的 60 天試用版軟體，體驗領先業界的端點防護功能：

http://www.symantec.com/endpoint-protection/trialware

參閱第三方評論並探索何以 Gartner 將賽門鐵克評等為端點防護平台神奇象限 (Magic Quadrant) 中的領導者：

http://www.symantec.com/endpoint-protection/news-reviews

請造訪我們的網站

http://enterprise.symantec.com 或 http://go.symantec.com/sep

關於賽門鐵克

賽門鐵克公司 (NASDAQ：SYMC) 是全球領先的網路安全公司，無論資料存放於何處，我們都能協助企業、政府機構及一般民眾保障他們最重要的資料安全。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。此外，全球有超過五千萬名使用者和家庭同樣也選擇採用賽門鐵克的諾頓產品套裝軟體，為家中及所有的裝置提供防護。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 www.symantec.com.tw。

台灣賽門鐵克股份有限公司

地址：台北市信義路五段 7 號台北 101 大樓 13 樓 A 室
電話：(02) 8726-2000
傳真：(02) 8726-2199
www.symantec.com/zh/tw

21320633-6 10/16