Symantec Endpoint Protection 的全新安全增強功能

肯・湯姆
產品行銷、端點安全

阿爾佩什・莫特
產品管理主管、端點安全

賽門鐵克端點用戶獲得增強的安全性和作業系統支持

安全世界不斷變化，有時比您想要的更快。人們現在可以在任何地方工作，不僅僅是在公司總部。自攜裝置(BYOD)已將數十億台設備添加到企業生態系統中。這就是為什麼賽門鐵克作為博通(Broadcom--美國股市代號：AVGO)企業安全部門，通過我們的端點安全解決方案繼續，成為您在此旅程中首選供應商。賽門鐵克端點安全，一個 SaaS 應用程式服務，提供了地球上最完整、整合性最佳的端點安全平台。作為地端、混合架構或雲端解決方案，單一代理程式的賽門鐵克端點平台可保護您的所有傳統和行動端點設備，並使用人工智慧 (AI) 優化安全決策。統一的雲端管理系統簡化了針對您的端點所有進階威脅的保護、偵測和回應。

我們最近與端點安全產品線管理負責人 Alpesh Mote 討論了支持我們旗艦 Symantec Endpoint Security 產品最新賽門鐵克端點安全版本 (14.3 RU1)。以下是我們談話中的一些亮點：

問：讓我們先談談新的 Symantec Endpoint Protection 14.3 RU1 版本中增強的安全效益；即「就地取材」攻擊的保護並阻止不受信任、不可移植的可執行文件。這些安全創新如何幫助我們的客戶？

答：攻擊者一直在使用非可攜式執行檔 (PE) 檔案，例如：嵌入惡意鏈接或實際惡意活動內容的 Office 檔案和 PDF 檔案，作為傳送工具來發起有針對性的目標攻擊。安全管理員必須查找並刪除這些檔案的每個副本，或者要求終端用戶不要開啟該檔案，都不是可靠或可擴展的解決方案。14.3 RU1 提供了一種可靠且易於使用的方法，管理員現在可以使用雜湊、大小和其他參數，**主動**阻止惡意的非可攜式執行檔 (PE) 檔案。

此外，在過去幾年中，賽門鐵克觀察到威脅格局已轉向使用日益複雜的技術進行針對性目標攻擊。其中包括攻擊者利用目標系統上已有的本機應用程式、工具和服務的「就地取材」策略。這允許攻擊者實現他們目標，而無需在磁碟上建立和部署他們的二進位檔案(binary)--可以說是無檔案(fileless)操作--或者與使用相同兩用工具的系統管理員日常工作融為一體。賽門鐵克端點保護(SEP) 具有多項新功能，可以更好地保護和預防利用「就地取材

」伎倆（包括勒索軟體和「供應鏈攻擊」）的針對性攻擊。通過 SEP 14.3 RU1，我們增強了我們的剖析技術，以防止威脅利用 Excel 等 Office 檔案進行攻擊，並**改進了對「就地取材」攻擊**中使用的常見檔案類型（例如：.LNK、.MSI、.PDF、.SCT、任務排程 XML）。我們還增強了對 Ryuk 和 Egregor 等勒索軟體的**行為檢測**，並優化了打包惡意軟體（.NET、VB 和 Delphi 打包程序）的評分啟發式保護。

> Symantec Endpoint Security 是一種 SaaS 應用程式，可提供全球最完整的整合式端點安全平台。

問：我看到賽門鐵克對許多作業系統進行了重大改進。讓我們從 macOS 代理程式開始。客戶喜歡此版本的哪些新元素？

答：在 ComputerWorld 最近發表的一篇文章中，IDC 證實 Mac 市場增長已達美國企業23%市占率。曾是為 Mac 提供保護的小眾功能現在正在成為主流。未受管理、未受保護的 Mac 給企業帶來了重大風險。這就是為什麼在 SEP 14.3 RU1 中我們 Mac 代理程式有重大改進的原因。此代理程式支持最新的 Apple Big Sur 作業系統。它還具有行為分析功來增強保護能力，分析好和壞的行為，以防止新的和未知的威脅。它包括一個新的入侵防禦引擎(IPS)，用於阻止網路的漏洞和惡意軟體/威脅。最新的代理讓 SOC 分析師能夠更好地了解進階威脅。您可以在我們的部落格上查看有關 macOS 保護的更多資訊：MacOS 上的賽門鐵克端點安全。

問：Linux 代理程式呢？賽門鐵克的客戶希望看到 RU1 有什麼亮點？

答：保護 Linux 資產對我們的客戶至關重要。大多數客戶將在服務主機使用 Linux，我們希望確保我們為客戶提供最好的安全性，以幫助保護他們環境中這些重要的核心關鍵系統。在 SEP 14.3 RU1 中，我們對 Linux 代理進行了重大更改。新的 Linux 代理是一個單一代理，可以從本地 Symantec Endpoint Protection Manager 或 Integrated Cyber Defense Manager 雲端控制台進行部署和管理。新代理引入了類似於 Windows 和 Mac 代理的 Symantec Endpoint Foundation，可提供機器學習和模擬器等進階防護技術。此版本還支持在 Linux 上使用 RPM 和 DEB 包進行部署，從而使管理員可以輕鬆部署和維護用戶端代理程式。

> 新的 Linux 代理是一個單一代理，可以從本地 Symantec Endpoint Protection Manager 或 Integrated Cyber Defense Manager 雲端控制台進行部署和管理。

問：賽門鐵克還為端點和用戶提供保護，使其免受基於 網頁(Web)的攻擊，請告訴我們更多相關資訊。

答：眾所周知，企業中很多用戶每天都會收到釣魚郵件或釣魚網址。網路釣魚和惡意分發網址(URL)被攻擊者用來分發惡意軟體，目的是獲取密碼和用戶/其他帳戶資訊。只需單擊網路釣魚電子郵件鏈接即可啟動勒索軟體攻擊。新整合的基於網頁(Web) 威脅防護和入侵防禦策略有助於防範網路釣魚 URL、殭屍網路命令與控制(C&C URL)、惡意軟體分發網址(URL)。

此功能獨特之處在於它匯集了我們在行業中首屈一指的兩項最強大的保護功能**入侵防禦**和我們的 **WebPulse 全局網頁(URL)情報資訊**。賽門鐵克的入侵防禦系統 (IPS) 是端點保護多重安全機制中的重中之重的功能，也是我們的第一道防線。幾乎每一次攻擊都是經由網路到達的-- IPS 在**入侵階段**提供早期保護，甚至在攻擊到達機器之前就阻止它。將這兩種技術結合在一起有助於增強我們的網路保護能力，通過利用網頁(URL)信譽資訊提供針對未知和已知威脅、漏洞利用和 C&C 流量的保護。

問：您能否詳細談談 Web 和雲端存取保護（網路流量重定向）與 SEP 14.3 RU1 的整合？

答：SEP 14.3 RU1 中的 Web 和雲端存取保護 (NTR) 將 Internet 流量轉發到 Symantec Web Security Services (WSS) 以進行基於策略的處理。這可以保護端點和用戶免受惡意站點 Web 的攻擊，並**阻止對違反公司政策的站點類別瀏覽**。

問：網頁和雲端存取的保護如何運作？

答：端點上的賽門鐵克代理使用來自賽門鐵克網頁安全服務 (WSS) 入口網站的 PAC 檔案或整合權杖。根據政策設置，來自端點的所有流量要將其重定向到 WSS 服務器進行分析、阻止或允許其繼續到達目的地。

這種整合的美妙之處在於所有這些功能都是通過單一代理提供的，即在端點上運行的同一個賽門鐵克代理程式。管理員不必部署和管理維護成本高昂的額外代理程式。

最危險和最具破壞性的威脅是你看不到的威脅。隨著針對性攻擊的複雜程度和數量不斷增加，企業需要減少分析師必須調查的事件總數，並確保回應者專注於最高優先等級的事件。SEP 14.3 RU1 代理是企業客戶解決方案的重要組成部分。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/product-insights/new-security-enhancements-symantec-endpoint-protection

關於作者

肯 • 湯姆

產品行銷、端點安全

肯 • 湯姆專注於賽門鐵克端點安全產品組合的是市場行銷工作。他在頂尖的網路和安全技術領先的公司，擁有超過 20 多年的產品管理和產品行銷經驗。

關於作者

阿爾佩什 • 莫特

產品管理主管、端點安全

阿爾佩什 • 莫特負責賽門鐵克旗艦端點安全產品的產品戰略和方向。自 2006 年以來，他一直從事網路安全工作，熱衷於了解客戶需求和提供創新產品。

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588