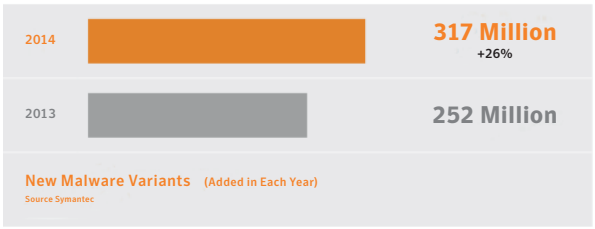
Symantec™ Data Center Security: Server 6.6

為您的 VMware 環境提供無代理程式型防惡意程式與網路 IPS

產品型錄：安全管理

威脅態勢概觀

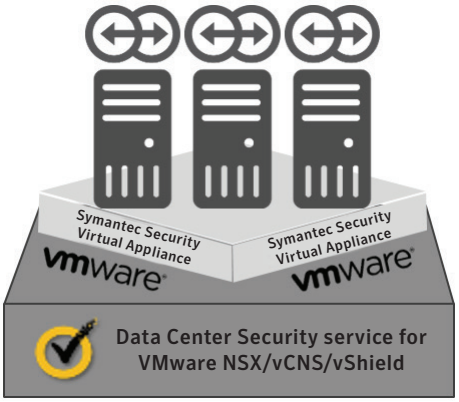
在 2014 年，有超過 3 億 1,700 萬支全新惡意程式被開發出來，相當於每天就有近 100 萬支獨特的惡意程式誕生。現在，惡意程式的總數已超過 17 億。



惡意程式作者會利用各種伎倆迴避偵測，其中一種方法就是在執行他們的程式碼之前，透過針對虛擬機器進行測式來找出安全研究人員。在 2014 年，就有高達 28% 的惡意程式具備「虛擬機器感知」能力。資料來源：第 20 期賽門鐵克網路安全威脅研究報告 (2015 年 4 月出版)

解決方案概述

Symantec™ Data Center Security (DCS): Server 6.6 可針對在 VMware NSX 和 vShield/vCNS 平台上執行的工作負載提供無代理程式型惡意程式防護、無代理程式型網路 IPS、以及檔案信譽服務。它可針對每一台主機提供單一執行個體安全服務，以保護該主機內的所有虛擬機器，進而加強資料中心的作業成效。



Symantec™ DCS: Server 6.6 也具備更新至 Unified Management Console (簡稱 UMC) 的功能，這是一種全新的網頁式主控台硬體裝置，可為所有 Data Cetner Security 產品提供一致性的管理體驗。客戶可使用 UMC 監控、登錄與設定 Symantec™ Data Center Security (DCS) 當中的功能、報表及產品。

Operations Director 和 Unified Management Console 是 Symantec™ Data Center Security 產品系列中推出的全新軟體導向安全功能。這些強化功能以下列核心原則為基礎：將安全機制內嵌於平台、整合和簡化單一功能技術，以及跨資料中心自動執行和協調安全機制。這些強化的功能可使安全措施跟上企業與 IT 作業的速度，進而提升運作效率並減輕嚴重的安全風險。

為何要選擇 Symantec™ Data Center Security: Server？

如果您的團隊想知道以下任一問題的答案，這就代表貴公司適合採用 Symantec™ Data Center Security: Server：

- 如何針對 NSX 和 vShield/vCNS 新建立的虛擬工作負載動態佈建應用程式層安全措施？
- 如何提供動態且有效運作的防惡意程式與網路 IPS 防護功能，而不致加重網路資源和應用程式效能的負擔？
- 如何佈建安全機制，以跟上業務與 IT 的速度？
- 如何在基礎架構與應用程式擴充時，水平擴充安全機制？
- 如何在需要最低限度的系統管理員訓練下，管理與保障我們公司資料中心的資產？
- 如何運用已規劃和現有的 VMware vShield/vCNS 及 NSX 投資來強化軟體導向資料中心的安全性？
- 如何降低掃描和定義檔更新 (例如掃描與更新風暴) 對系統資源的影響？

Symantec™ Data Center Security: Server 6.6 有哪些新功能？

- **針對在 VMware vShield/vCNS 平台上執行的工作負載提供無代理程式型惡意程式防護功能** – DCS: Server 6.6 透過直接在虛擬機器管理員整合來提供無代理程式型防惡意程式解決方案，因此就能將防惡意程式掃描工作的負擔移至安全虛擬硬體裝置（Security Virtual Appliance，簡稱 SVA）上，達到更高的效能與更高的訪客虛擬機器密度
- **自動部署 Security Virtual Appliance** – DCS 6.6 透過將可隨資料中心規模而擴充的 Security Virtual Appliance 自動部署至 VMware ESX，充分運用單一 SVA，同時為 VMware NSX 和 vShield/vCNS 提供威脅防護功能
- **網路威脅防護** – DCS 6.6 為網路防護新增了許多功能，可讓系統管理員管理白名單與黑名單。當 DCS 偵測到來自有問題的 IP 或網址的威脅時，會自動將原始資料來源列入黑名單
- **Operations Director（簡稱 OD）** – DCS 6.6 現在提供了立即可用的安全情報，可針對威脅的應變將安全協調工作自動化。該功能現在還隨附新增的 Rapid7 Nexpose 漏洞掃描工具。OD 還能搭配其他產品與作業工具整合性 SDK。
- **Unified Management Console（簡稱 UMC）** – UMC 是一項最新的網頁式主控台硬體裝置，可針對 Data Center Security 產品提供一致的管理體驗。客戶可使用 UMC 監控、登錄與設定 Symantec™ Data Center Security (DCS) 產品系列當中的功能、報表及產品。現在，它還能讓系統管理員自訂儀表板與圖表。DCS 6.6 也提供 Live Update 功能，可自動下載與更新 UMC 硬體裝置
- **延伸的平台支援能力**
  - vSphere 5.5/6.0 及 NSX 6.1.4
  - vCNS 5.5.4 及 vSphere 5.5/6.0

Symantec™ Data Center Security: Server 標準功能

- 無代理程式型惡意程式威脅防護。
  - 支援 VMware NSX 及 VMware vShield/vCNS (Non-NSX)，可針對在虛擬環境上執行的工作負載提供無代理程式型威脅防護功能
  - 在 vShield/vCNS (non-NSX) 上的防惡意程式功能結合了賽門鐵克的 Insight 信譽
  - 可同時為 vShield/vCNS 及 NSX 環境 (SVA) 自動部署安全虛擬硬體裝置，提供水平擴充的基礎架構
  - 群組化資產與防護政策
- 與 Symantec DeepSight 整合，可提供檔案和網址的信譽安全技術。
- 自動部署與佈建安全虛擬硬體裝置至叢集內的 ESX 主機。
- 在虛擬機器管理員層級整合，提供惡意程式感染的即時偵測與矯正功能。
- 利用同級最佳的安全防護技術提供隨時待命的安全機制
- 支援 VMWare vShield/vCNS 5.5.4 和 vSphere 5.5/6.0
- 屬於賽門鐵克廣大的遙測收集網路的一部分

客戶效益

- 內含強化的 vShield/vCNS 型虛擬硬體裝置支援能力
- 同時適用於 VMware NSX 與 vShield 的**單一安全虛擬硬體裝置** (SVA)
- **簡化的使用者介面**可同時為 VMware NSX 及 vShield/vCNS 提供豐富的使用者體驗與簡化的政策與資產管理功能
- **立即可用的儀表板**可提供資料中心的運作狀態及現況
- 透過無代理程式型防惡意程式與無代理程式型網路 IPS，**將虛擬機器與主機的網路與應用程式效能最佳化**
- 藉由採用單一定義檔更新**改善網路效能**
- **檔案與網址信譽服務**可與無代理程式型惡意程式防護服務相輔相成

- **自動部署虛擬硬體裝置**可在擴充工作負載之餘，將任何額外的維運開支成本降至最低
- 針對每一台主機提供單一執行個體安全服務，以**提升作業成效**
- 在虛擬機器管理員軟體提供安全機制， **免除為每一台虛擬機器掃描病毒的需要**
- **集中管理**病毒定義檔，不需要為每一台訪客虛擬機器更新病毒定義檔
- 在新的工作負載佈建期間提供**隨時待命的安全機制**，減少安全風險

Symantec™ Data Center Security 解決方案

Symantec™ Data Center Security 可讓企業強化他們的實體與虛擬伺服器、安全地轉換至軟體導向資料中心，並且跨公用與私有雲端環境提供以應用程式為中心的安全機制。

Symantec™ Data Center Security 產品系列包括：

Symantec™ Data Center Security: Server 利用無代理程式型防惡意程式、網路 IPS 及檔案信譽服務，針對 VMware 環境提供流暢的威脅防護。它可支援訪客機器內的隔離所功能，以便根據政策隔離可疑的惡意程式檔案並加以矯正。Symantec™ Data Center Security: Server Symantec™ Data Center Security: Server 會自動提供可水平擴充的安全虛擬硬體裝置 (SVA)，進而大幅節省維運開支成本。

Symantec™ Data Center Security: Monitoring Edition 可讓企業持續監控其實體與虛擬基礎架構以及公用 (AWS) 與私有 (OpenStack) 雲端的安全和遵循狀態。它結合了無代理程式型惡意程式碼防護與 IPS/IDS 監控、檔案完整性監控，以及組態監控功能。本產品的用途在於讓客戶將其安全作業與遵循監控和報告工作加以自動化和集中化。

Symantec™ Data Center Security: Server Advanced 可同時為實體與虛擬伺服器基礎架構提供安全偵測、監控及預防功能。Symantec™ Data Center Security: Server Advanced 除了針對虛擬與實體基礎架構和跨 AWS 與 OpenStack 雲端提供無代理程式型防惡意程式防護和安全監控之外，還能提供應用程式與受保護的白名單，以及精密的入侵偵測和預防；檔案、系統和系統管理員鎖定；以及檔案完整性和組態監控，以保護實體與虛擬伺服器。它也支援完全強化的 OpenStack Keystone。

Symantec™ Control Compliance Suite 可自動搜尋資產與網路、將安全評估工作自動化，以及計算和彙總 CVSS/CIS 風險評分。

利用 Control Compliance Suite，客戶即可啟用基本的安全檢疫功能，並獲得深入其安全、遵循和風險狀態的能見度。客戶可利用此情報來排定矯正工作的優先順序，並將安全資源的分配最佳化。

Symantec™ Protection Engine 可提供內容掃描、防惡意程式、疫情偵測、防垃圾郵件、深入分析與信譽服務，以及適合各種資料儲存方式 (如雲端儲存、NAS、電子郵件及 AWS) 的精密內容過濾技術。針對 NetApp NAS、Microsoft Exchange 和 Sharepoint 資料儲存區提供立即可用的支援能力，穩定的 SDK 則可針對其他資料儲存區提供自訂的整合性。

欲知更多資訊

請造訪我們的網站：

http://enterprise.symantec.com

About Symantec

賽門鐵克公司 (NASDAQ：SYMC) 是網路安全領域的全球領導廠商。我們運行全球規模最大的網路情報網之一，因而得以發現更多線上威脅，並保護更多客戶免於遭受新一代網路攻擊。無論最重要的資料存放於何處，我們都能協助公司、政府機構和個人妥善保存。

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

21347665-1 05/16