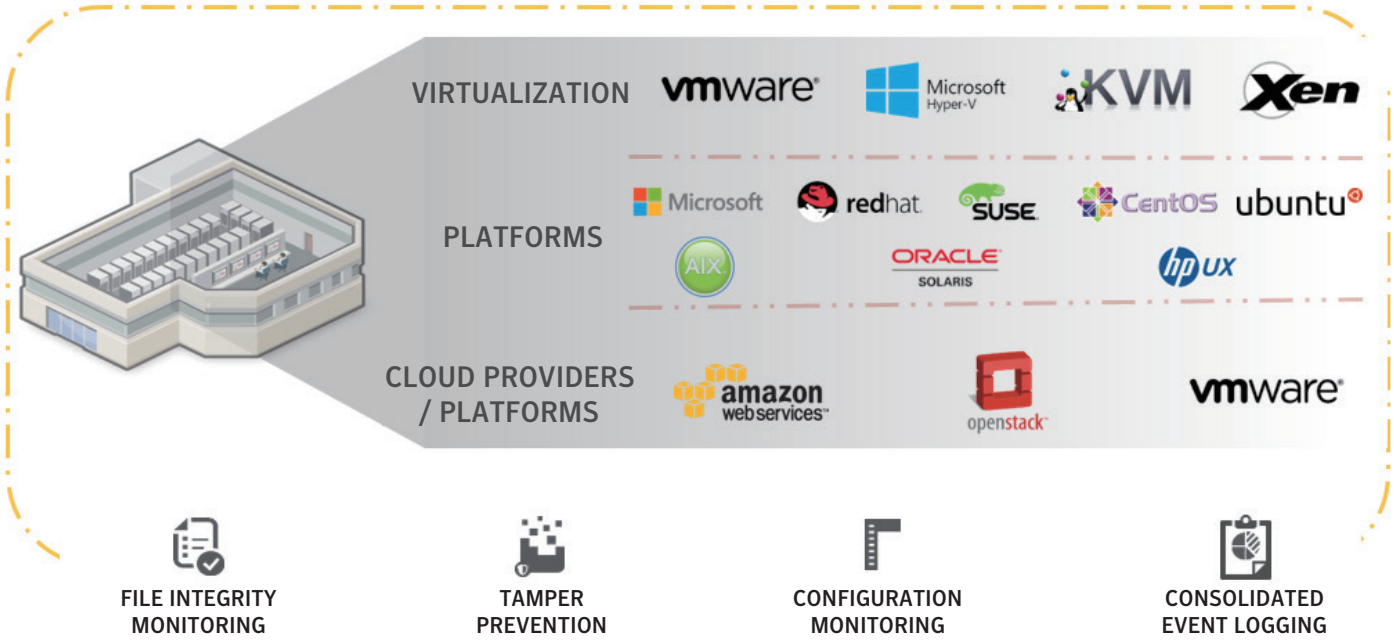
Symantec ™ Data Center Security: Monitoring Edition

針對實體與虛擬伺服器以及私有與公用雲端簡化不中斷的安全監控工作。

產品型錄：安全管理

解決方案概述

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) 雲端部署環境的安全和遵循狀態。



Symantec™ Data Center Security: Monitoring Edition 可同時為實體與虛擬伺服器提供立即可用的主機入侵偵測政策。它還將安全監控功能延伸到 Amazon Web Services (AWS) 以及 Openstack 雲端的所有模組。利用 Monitoring Edition，客戶就能監控檔案的完整性與組態、整合事件記錄，以及利用單一工具針對內部資料中心與雲端資料中心採用白名單和應用程式控制機制。

Symantec™ Data Center Security: Monitoring Edition 的客戶也能夠存取 Symantec™ Data Center Security: Server 提供的功能，包括：

- 無代理程式型防惡意程式
- 無代理程式型網路 IPS
- 直接與 VMWare 整合
- Operations Director
- Unified Management Console

如需更多資訊，請至以下網址參閱 Symantec™ Data Center Security: Server Datasheet

為何要選用 Symantec™ Data Center Security: Monitoring Edition？

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: Monitoring Edition：

- 如何跨實體與虛擬伺服器以及 AWS 與 OpenStack 雲端，即時且有效地在應用程式層或執行個體層偵測違反政策的情況及可疑活動？
- 如何在應用程式層或執行個體層有效地監控我們公司 AWS 與 Openstack 雲端部署環境的安全和遵循狀態？
- 如何涵蓋實體與虛擬伺服器以及 AWS 與 OpenStack 雲端，並簡化持續監控與遵循的報表作業？
- 如何涵蓋實體與虛擬伺服器以及 AWS 與 OpenStack 雲端即時偵測並且判別檔案的變更？
- 如何佈建安全機制，以跟上業務與 IT 的速度？

標準功能

- 跨實體與虛擬伺服器的安全監控功能包括：
  - 即時的檔案完整性監控：即時判別對檔案的變更，包括變更的人員和變更的內容
  - 組態監控：即時判別違反政策的情形及可疑活動
  - 整合的事件記錄：整合和轉送記錄以供長期保存、報告和蒐證分析
  - 檔案與系統竄改防護功能：鎖定組態、設定值及檔案
  - 儀表板：輕鬆判別異常事件活動，並監控您的重要效能指標
- OpenStack 資料中心基礎架構的安全監控功能包括：
  - 組態變更：使用即時檔案完整性監控功能來監控對組態檔案進行的變更
  - Keystone 程式檔案：監控模組中的 Python 檔案，以避免重要系統服務的檔案遭到竄改
  - Keystone 資料：嚴密監控使用者帳戶、角色和分租共用資料的變更動作
  - 存取監控：透過網頁式介面監控使用者的存取動作
- AWS 公用雲端與混合型雲端 (VPC) 的安全監控功能包括：
  - 安全組態監控
  - 檔案完整性監控
  - 針對內部資料中心與雲端資料中心以應用程式白名單控制
  - 透過 REST API 提供跨雲端環境的安全自動化
- Symantec™ Data Center Security: Server 當中提供的特色與功能包括：
  - 無代理程式型防惡意程式、無代理程式型網路 IPS 及檔案信譽服務。
  - 自動部署安全虛擬硬體裝置 (Security Virtual Appliance) 並佈建至叢集伺服器內的的 ESX 主機。
  - 網路型威脅偵測與防護 (網路 IPS)。
  - Operations Director 可將剛建立的工作負載 (workload) 之安全佈建自動化，並加以協調。
  - Unified Management Console (簡稱 UMC) 能夠跨所有 Data Center Security 產品提供一致性的管理體驗。

客戶效益

- 能夠跨實體與虛擬伺服器、以及 AWS 與 OpenStack 雲端，即時在應用程式或執行個體層有效判別違反政策的情形及可疑活動的單一工具。
- 簡化在應用程式層或執行個體層監控 AWS 與 Openstack 雲端部署的安全和遵循狀態，並簡化其遵循報告作業。
- 跨實體與虛擬伺服器以及 AWS 與 OpenStack 雲端即時偵測並判別對檔案進行的變更。
- 透過無代理程式之防惡意程式與無代理程式之網路 IPS，將虛擬機器與主機的網路與應用程式效能最佳化。
- 針對每一台主機提供單一執行個體安全服務，以保護所有虛擬機器，進而提升作業成效。
- 在新的工作負載 (Workload) 佈建期間提供隨時待命的安全機制，減少安全風險。
- 監控並保護實體與虛擬資料中心。
- 功能完備的 REST API 提供了與所有主控台動作相對應的

應用程式開發介面 (API)，可以實現完整的內部與外部雲端自動化。
- 簡化混合型資料中心基礎架構的持續監控與遵循報告作業，以實現網路安全及遵循能力。

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** 可為 VMware 主機本身和虛擬機器提供無代理程式之防惡意程式、無代理程式之網路 IPS、虛擬機器內的隔離所功能以及檔案信譽服務。它能夠與 VMware vCenter、VMware NSX、Palo Alto Networks Next Generation Firewall 及 Rapid 7 Nexpose 整合，在工作負載 (Workload) 的整個生命周期中將應用程式層安全機制自動化並加以協調。

Symantec™ Data Center Security: Monitoring Edition 可同時提供實體與虛擬伺服器基礎架構的安全偵測及監控功能。除了提供無代理程式型防護功能外，Symantec™ Data Center Security: Monitoring Edition 還結合了無代理程式之惡意程式碼防護，以及入侵偵測、檔案完整性和組態監控功能。利用 Symantec™ Data Center Security: Monitoring Edition，客戶還可監控採用 OpenStack 的資料中心，包括組態變更、存取監控和 Keystone 資料。

Symantec™ Data Center Security: Server Advanced 可透過提供 (1) 應用程式與受保護的白名單 (2) 精細的入侵偵測與預防 (3) 檔案、系統與系統管理員鎖定功能 (4) 檔案完整性與組態監控，同時保護內部部署、混合型環境和雲端資料中心的實體與虛擬伺服器。藉由針對最常見的資料中心應用程式採用立即可用的監控及強化功能，Data Center Security: Server Advanced 可協助將所需的時間與工作減至最少，並降低作業成本。利用針對所有 OpenStack 模組的檔案完整性監控功能和完整強化的 Keystone 身分服務模組，保護您以 OpenStack 為基礎的資料中心。

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。

欲知更多資訊

請造訪我們的網站：

http://enterprise.symantec.com

關於賽門鐵克

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

21347664-1 05/16