Symantec™ Data Center Security: Server & Server Advanced

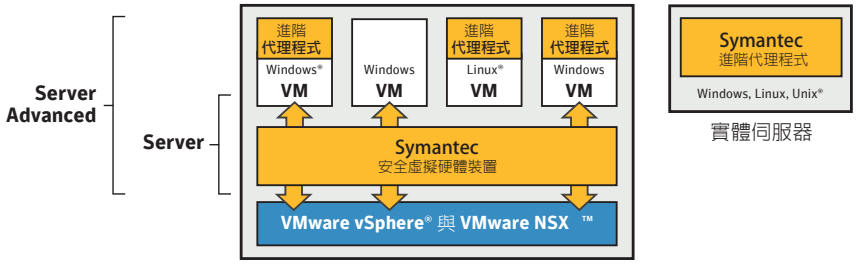
適用於虛擬及實體伺服器的最強防護

產品型錄：資料防護及安全管理

解決方案說明

Symantec Data Center Security: Server & Server Advanced 是一套能為資料中心伺服器提供安全性的全新賽門鐵克產品。

- **Symantec Data Center Security: Server** 能透過安全虛擬硬體裝置，提供適用於 VMware® 基礎架構的無代理防惡意程式防護功能，同時還能針對軟體導向資料中心 (SDDC) 提供安全政策協調功能及自動化工作流程。
- **Symantec Data Center Security: Server Advanced** 透過結合前身為「Critical System Protection」的技術，擴充了 Symantec Data Center Security: Server 的功能。Server Advanced 版本能透過低系統衝擊的虛擬機器代理程式，提供精細的政策式控制機制，以監控和防護異質化實體與虛擬伺服器環境。



Symantec Data Center Security: Server & Server Advanced 概述

為了保護實體與虛擬伺服器，過去 IT 專業人員仰賴的是傳統的防護技術，例如防毒程式。儘管這些技術仍然是最基本的防禦和保護層，今日的威脅態勢確實需要強化即時和主動式的安全功能，為伺服器提供更足夠的防護能力，以滿足每個系統對於逐漸提高的機密性、整合性及可用性要求。若無法為每一台獨一無二的伺服器提供最佳化的安全性，包括：網頁、檔案、應用程式或資料庫，企業就仍將使資料中心暴露於風險之中。

為軟體導向的資料中心提供安全應變能力

虛擬資料中心具備高度的彈性，而且關聯的虛擬機器也不斷在變動。為了能確保安全控制功能在這種環境中仍然可以正常運作，Data Center Security: Server & Server Advanced 運用了 VMware NSX 平台延伸性和 Service Composer 整合性，發揮基礎架構中每個細節的惡意程式防護功能，例如，每部主機單一執行個體安全虛擬硬體裝置，能夠強制執行每部訪客虛擬伺服器的專屬安全政策。隨著虛擬機器在主機之間移動時，安全政策也會自動地如影隨形。

主要功能包括：

虛擬資料中心策略

- 無代理程式型防惡意程式以 Symantec Insight™ 為後盾，適用於 VMware 基礎架構中的虛擬伺服器；
- 自動為主機佈建安全虛擬硬體裝置，並且可協調整個軟體導向資料中心內所有的安全政策
- 提供所有 VMware 合作夥伴協同合作生態系統的自動化安全工作流程

伺服器防禦策略

- 以應用程式為中心的安全模式：從依照不同技術設定政策的方式，轉變為以應用程式為中心的模式，以簡化伺服器強化作業
- 受防護應用程式白名單：預先建立的應用程式設定檔能加強嚴格的預設拒絕執行控制機制
- 沙箱技術及流程存取控制：對執行中的流程套用額外的控制機制，以防禦新型態威脅的攻擊

Symantec

防止伺服器出現零時差漏洞及遭受目標式攻擊

伺服器經常在資料洩漏的入侵、搜尋和擷取階段中，遭到網路罪犯鎖定。現今用來對付伺服器的技巧，包含從精細的滲透技巧到系統管理人員無心的設定錯誤。Data Center Security: Server Advanced 除了能讓企業控制惡意內部員工濫用與系統設定錯誤，還能強化伺服器、將應用程式沙箱化，減少修補工作和漏洞攻擊。藉由強化資料中心，就能阻止進一步的滲透，並避免敏感資料外洩。

減少新舊作業系統的修補程式作業

將軟體修補程式套用到新舊作業系統，雖然可改善安全態勢，但同時也會造成系統停機。此外，為停產的作業系統支付延長支援的費用可能非常昂貴而無法繼續。Data Center Security: Server Advanced 能降低與舊版系統支援相關的維護成本，並且在修補程式發佈週期間保護系統。客戶能藉由強化新舊系統的應用程式與作業系統，確保資料中心具備最高的安全性，系統具備最高的可用性。

取得 IT 遵循狀態的即時能見度

為遵循如 PCI 資料安全標準 3.0 (PCI DSS) 和其他標準規定，企業必須定期監控其環境，以瞭解是否發生違反政策並建置補償性的控制機制。Data Center Security: Server Advanced 能夠在單一解決方案中讓客戶執行即時監控、合併事件記錄以製作報表與分析，同時透過精細的政策導向控制機制，避免進一步違反政策，進而以集中化的解決方案展現遵循能力。

為 VMware 環境提供完善的防護

在虛擬環境中，應用程式與作業系統所受到的網路攻擊，與實體環境是完全相同的。此外，虛擬機器管理員軟體和管理伺服器層級所面臨的風險更需要防護及監控功能。考量虛擬環境中的安全性時，務必要選擇能在整個虛擬架構中抵禦內部員工風險與外部威脅、且不會影響效能的技術。Data Center Security: Server 已最佳化，能防護及監控 VMware vSphere 5.x。運用以最新 vSphere 強化指南為基礎、立即可用的政策，就能讓客戶在管理伺服器、虛擬機器管理員軟體和虛擬機器上完善保護其環境。

伺服器防禦策略

- 目標式預防政策：這項單鍵操作的預防政策能套用至資料外洩的情境，或做為從監控改為預防的方式。
- 主機防火牆：控制伺服器的入埠與離埠網路流量
- 預防檔案與系統被竄改：鎖住組態、設定值與檔案
- 應用程式與裝置控制：鎖住組態設定值、檔案系統與抽取式媒體的使用
- 補償性的 HIPS 控制機制：使用政策導向的最低權限存取控制，限制應用程式與作業系統的行為

伺服器偵測策略

- 即時檔案完整性監控：即時識別對檔案的變更，包括進行變更的人員與變更的內容
- 組態監控：即時識別違反政策的狀況與可疑活動
- 合併的事件記錄：合併並轉寄記錄，以進行長期保留、報告和鑑識分析

評估及法規遵循

- IT 分析 (ITA) 多維模型整合性：運用彈性且強化的儀表板功能，強化現有報表功能，達到更深入的能見度

關於賽門鐵克

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策略性整合式解決方案，在端點、雲端和基防架防中有效地抵而最複雜的攻擊。賽門鐵克經營的安全防報網是全球防防最大的民間防報網路之一，防此能成想偵測最進防的威脅，進　提供完善的站護善更。
若想瞭解更t　資施，請提訪原廠網瞭 https://www.broadcom.com/solutions/integrated-cyber-defense

Symantec™