

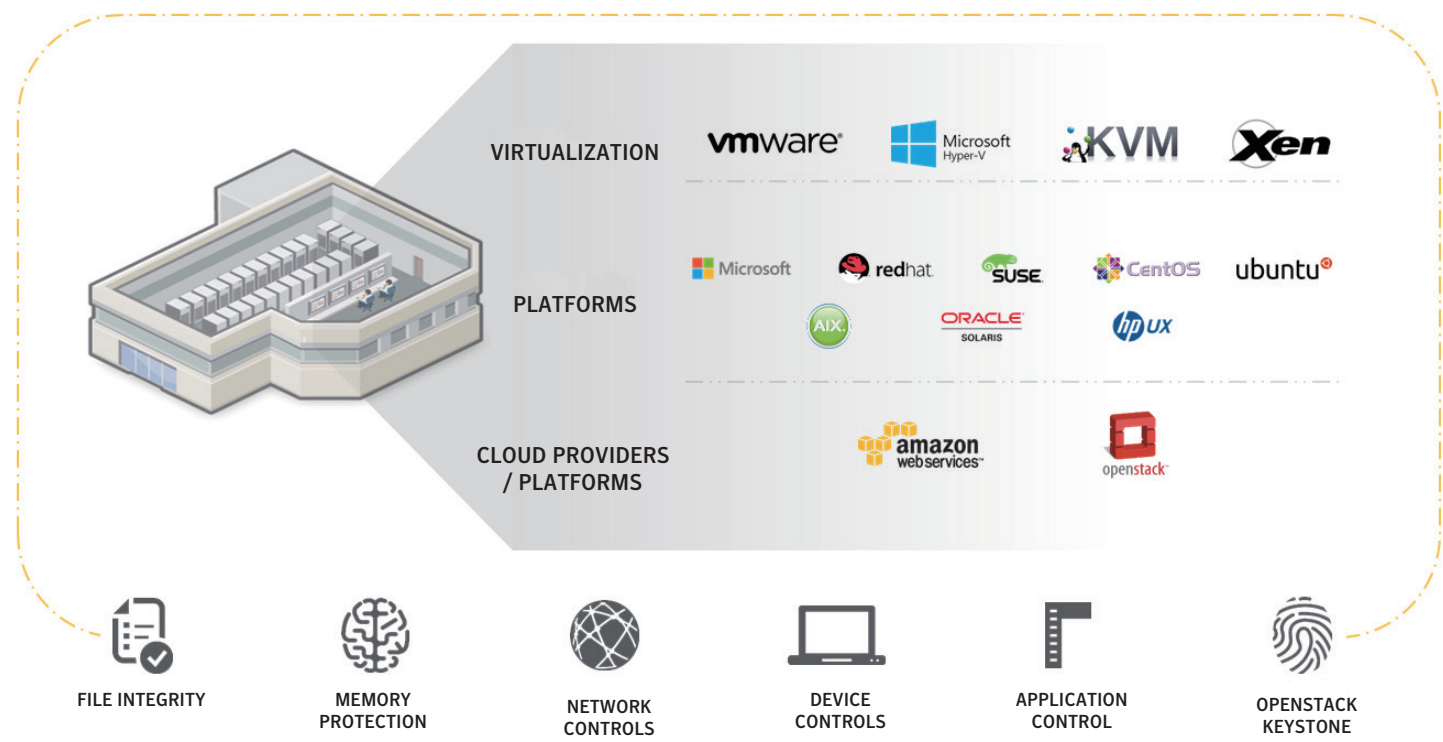
Symantec™ Data Center Security: Server Advanced

針對進階威脅的防護與強化

產品型錄：安全管理

解決方案概述

Symantec™ Data Center Security: Server Advanced 可提供完整的伺服器防護功能。完整的應用程式控制功能可在今日異質化的私有/公用雲端資料中心內，提供細微的區段分隔、防止系統管理員權限升級、降低修補程式的風險以及零時差威脅防護功能。



您是否能夠：

- 防護和強化您的異質化虛擬與實體伺服器環境？
- 防護與強化在老舊與終止支援 (EOL) 的平台上執行的重要應用程式？
- 有效地提供安全機制，並移轉已終止支援的伺服器平台？
- 迅速因應重大漏洞與未經授權的應用程式組態變更？
- 保護貴公司的重要伺服器基礎架構，避免零時差威脅和最新漏洞？
- 保護您的 OpenStack Keystone 建置環境？
- 在貴公司的 AWS 和 OpenStack 雲端部署環境中執行與監控應用程式層與執行個體層的安全機制？
- 針對剛建立的實體與虛擬工作負載快速佈建以應用程式為中心的安全強化措施？
- 將安全佈建與強化功能嵌入貴公司的 IT 流程中？

客戶效益

- 牢不可破的安全性。賽門鐵克的 Data Center Security: Server Advanced 連續五年在內華達州拉斯維加斯市舉辦的黑帽駭客年會「奪旗」入侵挑戰中，創下牢不可破的佳績。
- 確保老舊平台或已終止支援的平台上執行之未經修補的應用程式與系統安全。
- 利用立即可用的安全情報將威脅應變工作自動化，以防止重大漏洞和未經授權的應用程式組態變更。
- 不受虛擬化技術限制以及廣泛支援各種平台，這代表客戶可以確保工作負載的安全不受其所在地點的影響，同時還能保護包含無法修補之老舊系統在內的整個資料中心。
- 運用主機型入侵偵測 (HIDS)、主機型入侵預防 (HIPS) 與最低權限存取控制的組合，監控及保護實體與虛擬資料中心。功能完備的 REST API 可針對所有主控台活動提供對應的 API，藉以實現完整的內部與外部雲端自動化。
- 由終止支援的平台安全且符合作業成本效率地移轉。
- 減少對於新舊系統的修補動作。
- 針對公用和混合雲端部署環境提供應用程式與執行個體層的安全性。
- 持續監控資料中心基礎架構，以實現網路安全及遵循能力。

6.6 版中有哪些新功能？

- 利用更新的網頁式使用者介面精簡操作工作
- 利用最新的應用程式導向之安全群組來降低運作成本

- 利用引導式調校工作流程，將推出強化功能的時間減至最少
- 利用應用程式搜尋與強化功能減少強化您 Unix 工作負載安全性所需的時間；Advanced Resilient Unix 代理程式則可在您的環境演進時提供防護
- 平台支援能力：Ubuntu 14.0.4

Server Advanced 也包含了 Monitoring Edition 6.6 和 Server 6.6 當中所有的新功能：

- 監控 OpenStack 資料中心基礎架構
- 利用儀表板輕鬆判別異常事件活動，並監控您的重要效能指標
- 為 VMware NSX 上的虛擬伺服器提供無代理程式型網路 IPS
- 在 vCNS/vShield 平台上提供防惡意程式功能
- 在 NIPS 中支援 IPv6 及白名單/黑名單
- 新增的平台支援能力：vSphere 5.5/6.0、NSX 6.1.4、vCNS 5.5.4

標準功能

- **立即可用的 Host IDS 與 IPS 政策**：針對 Windows® 環境預設建立的政策可監控並防止可疑的伺服器活動。
- **沙箱技術與程序存取控制 (PAC)**：運用全方位的 IPS 防護功能來防範新型威脅。
- **主機防火牆**：控制往來伺服器的入埠與離埠網路流量。
- **補償性的 HIPS 控制**：使用政策導向的最低權限存取控制來限制應用程式與作業系統行為。
- **預防檔案與系統竄改**：鎖定組態、設定值及檔案。
- **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。

Symantec™ Data Center Security 解決方案概述

Symantec™ Data Center Security: Server 可為 VMware 主機和虛擬機器提供無代理程式型防惡意程式、無代理程式型網路 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型惡意程式碼防護，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。

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>

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