趨勢科技™

DEEP SECURITY

實體、虛擬與雲端伺服器的全方位防護平台

虛擬化及雲端運算已徹底改變了今日的資料中心，但許多企業在從傳統實體環境移轉至以虛擬化和雲端運算為主的現代化資料中心時，卻仍使用傳統式安全防護。在虛擬化環境當中，傳統式防護不僅將提高營運的複雜度，更會降低主機效能與虛擬機器（VM）的使用密度；還可能造成防護上的漏洞，影響企業將核心關鍵系統移轉至雲端環境的信心，無法享受靈活與低成本的效益。最重要的，傳統式防護會阻礙現代化資料中心的虛擬化及雲端運算發揮應有的投資報酬（ROI）。

防範資料外洩和業務中斷

趨勢科技 Deep Security™ 是專為保護您資料中心與雲端工作、防範資料外洩與業務中斷而設計，提供軟體與軟體服務兩種部署方式。Deep Security 能協助企業有效率地防範虛擬與雲端環境的安全漏洞，進而達成法規遵循要求。

從單一整合式主控台管理的多功能防護

Deep Security 採用各種整合式模組，包括惡意程式防護、網站信譽評等、防火牆、入侵防護、一致性監控以及記錄檔檢查，來確保伺服器、應用程式與資料的安全，涵蓋實體、虛擬及雲端環境。Deep Security可透過多功能單一代理程式來部署至所有環境，並藉由單一管理儀表板來執行所有功能，簡化安全防護作業。

透過密切的整合將防護政策延伸至雲端環境

Deep Security能與各種雲端平台密切整合，包括 Amazon Web Services (AWS)、Microsoft Azure 以及 VMware vCloud Hybrid Service，讓您將資料中心防護政策延伸至雲端。Deep Security藉由各種跨環境而最佳化的功能，讓企業和服務供應商能為使用者提供個別而安全的分租共用雲端環境。

企業主要問題

虛擬桌面防護

- 透過全方位的無代理程式安全防護來維持效能與系統整合密度，提供專為 VDI 環境設計的最大防護。

虛擬修補技術

- 預先防止漏洞遭到攻擊，消除緊急修補、減輕頻繁修補程式部署的營運困擾，以及系統停機所帶來的昂貴成本。

法規遵循

- 可達成並證明符合各種法規要求，包括：PCIDSS3.0、HIPAA、HITECH、FISMA/NIST、NERC、SAS70等等。

採用專為現代化資料中心設計的防護來加速雲端和虛擬化的投資報酬

虛擬化防護

Deep Security 能保護虛擬桌面和伺服器，防範零時差（zero-day）惡意程式和網路攻擊，同時能消除資源利用率不佳與緊急修補對營運所造成的衝擊。

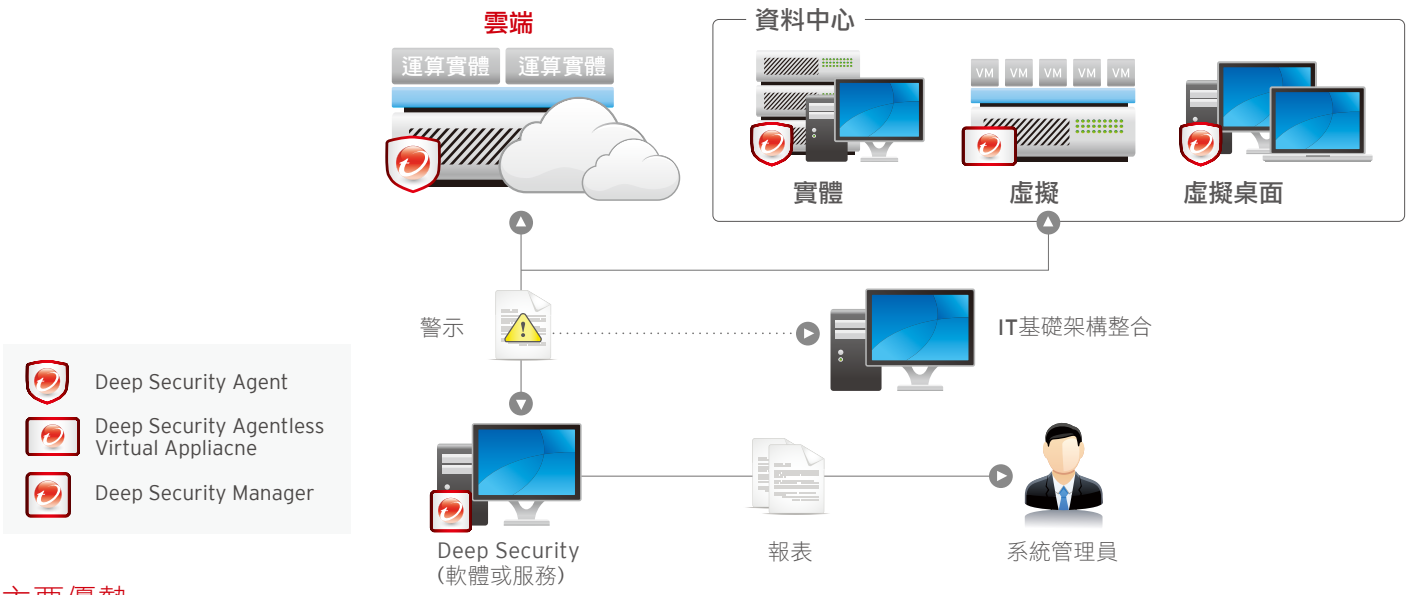
雲端防護

Deep Security 能讓服務供應商及現代化資料中心提供一個安全的分租共用雲端環境，將防護政策延伸至雲端，透過一致的環境感應式政策來集中管理。

整合式伺服器防護

Deep Security 將所有個別伺服器防護功能集中至單一全方位整合彈性平台，為實體、虛擬與雲端伺服器提供最佳防護。

同時掌控實體、虛擬與雲端的安全防護



主要優勢

加速虛擬化及雲端的投資報酬

- 相較於傳統，採用無代理程式的惡意程式防護，可提高虛擬機器密度並提升資源利用率與管理效率。
- 採用多功能單一防護代理程式來增加額外的彈性與縱深防禦功能。
- 藉由虛擬化監管程式（hypervisor）層次的避免重複掃瞄技術，提供無可匹敵的效能。
- 與雲端平台整合，包括 AWS、Microsoft Azure 及 VMware vCloud Hybrid Service，讓企業透過一致的環境感應式防護政策來管理實體、虛擬及雲端伺服器。
- 讓服務供應商為客戶提供一個安全的公有雲，透過分租共用架構與其他承租戶隔離。
- 提供自動擴充的公用運算及自助式服務，利用軟體定義的資料中心來支援企業的靈活度。
- 透過 Deep Security 與 VMware 的密切整合，自動偵測新增的虛擬機器並且套用環境感應式政策，讓資料中心和雲端維持一致的安全性。
- 藉由與 VMware NSX™ 整合，Deep Security 就能進一步延伸軟體定義資料中心精密切割的效益，讓防護政策和防護功能自動跟隨著虛擬機器，不論虛擬機器移到哪裡。

避免資料外洩和業務中斷

- 以最小的效能負載即時偵測並清除虛擬伺服器上的惡意程式。
- 攔截嘗試移除或破壞防護軟體以躲避偵測的惡意程式。
- 防堵已知及未知的網站應用程式及企業應用程式和作業系統漏洞。
- 在偵測到可疑或惡意活動時發出警示並觸發主動預防措施。
- 追蹤網站信譽，利用趨勢科技全球網站信譽評等資料庫的威脅情報來防止使用者誤觸已遭感染的網站。
- 利用趨勢科技的全球威脅情報來偵測及攔截殭屍網路與鎖定目標式攻擊的C&C通訊。

徹底降低營運成本

- 透過集中管理的單一代理程式或虛擬裝置，消除部署多種用戶端軟體的成本。
- 與趨勢科技、VMware 及企業目錄服務的管理主控台密切整合，降低複雜度。
- 防堵漏洞，填補式程式碼的安全性修正，減少非定期性修補程式的部署成本。
- 將重複性和耗費人力的安全作業自動化以降低管理成本，減少安全警示誤判，實現資安事件回應流程。
- 採用雲端事件白名單與可信賴事件清單，大幅降低檔案一致性監控的複雜度。
- 透過建議掃瞄來偵測漏洞及軟體變更，進而提供漏洞防護。
- 採用更輕盈、更機動的智慧型代理程式來提升營運效率，減輕部署難度，讓資源在資料中心與雲端之間做最有效的分配。
- 配合您的政策進行防護，減少專為配合單一安全控管所需的資源。
- 集中管理各項趨勢科技防護產品，簡化管理作業，集中產生多種安全控管報表，減少產生個別產品報表的麻煩。

實現符合成本效益的法規遵循

- 採用單一合乎成本效益的整合式解決方案來達成重大法規要求，如：PCI DSS 3.0 以及 HIPAA、HITECH、NIST 和 SAS 70。
- 提供稽核報表，記載已防止的攻擊清單並提供政策遵循狀態。
- 減少稽核作業的準備時間與人力。
- 支援內部遵法規計劃，提升內部網路活動的掌握度。
- 採用通過 Common Criteria EAL 4+ 認證的技術。

DEEP SECURITY 平台模組

惡意程式防護與網站信譽評等

- 與 VMware vShield Endpoint API 整合，完全不需在虛擬機器內安裝任何元件就能為 VMware 虛擬機器提供病毒、間諜程式、木馬程式以及其他惡意程式防護。
- 提供一套惡意程式防護代理程式，將防護延伸至實體、虛擬及雲端伺服器，包括AWS、Microsoft及VMware 環境。
- 可透過 VMware ESX 層級的快取與避免重複掃瞄技術來提升效能。
- 讓防護作業最佳化，避免傳統防護產品在執行全系統掃瞄與病毒碼更新時常見的效能風暴。
- 將惡意程式與核心作業系統及防護元件隔離，防止虛擬環境下的防護遭到精密攻擊竄改。
- 與趨勢科技 Smart Protection Network™ 全球威脅情報整合，透過網站信譽評等來強化伺服器與虛擬桌面的防護。

入侵防護

- 檢查所有內送與外送的流量，藉此偵測通訊協定上的錯誤、違反政策的情形、或是疑似攻擊的可疑內容。
- 藉由虛擬修補技術自動防堵已知但尚未修補的漏洞，防止漏洞遭到無限制利用，幾分鐘就能將防護配送至數千台伺服器，而且不必重新開機。
- 保護網站應用程式和這些程式所處理的資料，符合遵規要求(PCIDSS第6.6條)。
- 防止SQL資料隱碼攻擊(SQL injection)跨網站攻擊(cross-site scripting)以及其他網站應用程式漏洞。
- 內建支援主流作業系統與100多種應用程式，包括：資料庫、網站、電子郵件、FTP 等伺服器在內。
- 提升對所有網路存取應用程式的掌握與掌控。

雙向主機式防火牆

- 縮小實體、虛擬與雲端伺服器的攻擊面，提供精細的過濾規則與針對個別網路的政策，並且自動偵測所有 IP 通訊與訊框類型的來源位置。
- 集中管理伺服器防火牆政策，內含常見伺服器類型的範本。
- 防止阻斷服務攻擊，偵測探查式掃瞄。
- 提供主機防火牆事件記錄，提供法規遵規與稽核報表，這對公有雲端部署環境尤其重要。

一致性監控

- 監控重要的作業系統與應用程式資料，例如：檔案、目錄、系統登錄機碼與數值等等，即時偵測並通報惡意和非預期的變更。
- 採用 Intel TMP/TXT 技術來執行虛擬化監管程式 (hyper visor) 的一致性監控，發掘任何未經授權的變更，將安全防護和法規遵循延伸至虛擬化監管程式層次。
- 使用可信賴事件標籤來減輕管理負擔，自動複製類似事件的應對行動，涵蓋整個資料中心。
- 簡化管理，透過趨勢科技認證安全軟體服務 (Certified Safe Software Service) 的自動化雲端白名單，大幅降低已知正常的事件數量。

記錄檔檢查

- 蒐集並分析全資料中心的作業系統與應用程式記錄檔，從中發掘可疑行為、資訊安全事件、系統管理事件等等，支援100多種記錄檔格式。
- 促進法規遵循 (PCIDSS第10.6條)，更容易發現隱藏在多筆記錄內的重要安全事件。
- 可將事件傳送到一個 SIEM 系統或是中央記錄伺服器，在此進行關聯分析、報表與歸檔。

Deep Security 讓我們去除了伺服器上的另一套防毒軟體...這套軟體占用了大量的記憶體，而且掃瞄時會消耗大量 CPU 資源。Deep Security 完全沒有這方面的問題。

Blaine Isbelle美國加州柏克萊大學資訊服務科技部門系統管理員

部署與整合

利用現有的IT和資訊安全投資快速完成部署

虛擬桌面防護

- 與 vShield Endpoint、VMsafe™ API以及VMware vCenter 整合，可採用虛擬裝置方式快速部署在 ESX 伺服器上，立即自動保護 vSphere 虛擬機器。
- 提供詳細的伺服器層級安全事件，並可傳送至SIEM系統，如：ArcSight、Intellitactics、NetIQ、RSA Envision、Q1Labs、Loglogic 以及其他系統 (透過不同整合選項)。
- 可與企業目錄服務整合，如：Microsoft Active Directory。
- 代理程式軟體可輕鬆透過標準的軟體配送機制來部署，例如 Chef、Puppet、AWSOpsWorks、Microsoft System Center Configuration Manager (SCCM)、Novell ZENworks 以及 Symantec Deployment Solution。

雲端服務夥伴認證

「Trend Ready for Cloud Service Providers」是一項針對雲端服務合作夥伴(CSP)的全球測試認證計劃讓雲端廠商證明其服務與趨勢科技領先業界的雲端安全防護解決方案能夠相互通用。

平台架構

Deep Security 虛擬裝置。自動在後台強制貫徹 **VMware vSphere** 虛擬機器防護政策，提供無代理程式的惡意程式防護、網站信譽評等、入侵防護、一致性監控以及防火牆保護，還可搭配 **Deep Security** 代理程式來提供記錄檔檢查亦達到縱深防禦效益。

Deep Security 代理程式。部署在受保護的伺服器或虛擬機器上的輕量軟體元件，可強制貫徹資料中心的防護政策(惡意程式防護、入侵防護、防火牆、一致性監控以及記錄檔檢查)。它可透過市場主流的管理工具來自動部署，如 **Chef**、**Puppet** 和 **AWS OpsWorks**。

Deep Security 管理程式。強大的集中管理主控台提供了角色導向的管理與多層式政策繼承功能，提供細緻的控管。建議掃瞄與事件標籤等作業自動化功能，可簡化日常的防護管理工作。分租共用的架構可支援不同承租戶之間的政策隔離，並且讓個別承租戶系統管理員分擔防護管理責任。

全球威脅情報。**Deep Security** 也與趨勢科技 **Smart Protection Network** 整合，藉由不斷評估及關聯分析各種網站、電子郵件來源以及檔案的全球威脅和信譽評等情報，為最新的威脅提供即時防護。

平台架構

Microsoft® Windows ®

- Windows XP, Vista, 7, 8, 8.1 (32-bit/64-bit)
- Windows Server 2003 (32-bit/64-bit)
- Windows Server 2008, 2008 R2, 2012, 2012 R2 (64-bit)
- XP Embedded

Linux

- Red Hat® Enterprise 5, 6 (32-bit/64-bit)[1]
- SUSE® Enterprise 10, 11 (32-bit/64-bit)[1]
- CentOS 5, 6 (32-bit/64-bit)[1]
- Amazon Linux[1]
- Ubuntu 10, 12, 14.04 (64-bit)[1]
- Oracle Linux 5, 6 (32-bit/64-bit)[1]
- CloudLinux 5, 6 (32-bit/64-bit)[1]

Oraclesolaris™

- OS: 9, 10, 11 (64-bit SPARC), 10, 11 (64-bit x86)[2]
- Oracle Exadata Database Machine, Oracle Exalogic Elastic Cloud and SPARC Super Cluster via the supported Solaris operating systems

UNIX

- AIX 5.3, 6.1 on IBM Power Systems[3]
- HP-UX 11i v3 (11.31)[3]

虛擬化

- VMware®: 5.1/5.5/vCloud Networking and Security 5.1, View 4.5/5.0/5.1, ES X 5.5
- Citrix®: XenServer[4]
- Microsoft®: HyperV[4]

1.惡意程式防護僅支援隨選掃瞄。 2.不提供惡意程式防護。 3.不提供惡意程式防護，僅AIX提供防火牆和入侵防護。
4.僅能透過 **Deep Security** 代理程式提供防護。

主要認證與策略聯盟

- Amazon 高級技術合作夥伴
- Red Hat Ready 認證
- Cisco UCS 認證
- common criteria eAl 4+
- EMC VSPEX 認證
- HP 業務合作夥伴
- Microsoft Active Protection Program 會員
- 微軟認證合作夥伴
- NetApp FlexPod 認證
- Oracle 合作夥伴
- PCI Suitability Testing for HIPS 認證 (NSS Labs)
- VCE Vblock 認證
- VMware 虛擬化認證

amazon web services Partner Network
ADVANCED TECHNOLOGY PARTNER

vmware

Microsoft Azure

TREND MICRO READY CLOUD SERVICE PROVIDER

TREND MICRO™

Securing YourJourney to the Cloud

趨勢科技官方網站:www.trendmicro.com.tw
趨勢科技企業專線:(02)2378-2666