趨勢科技

Deep Security™

實體、虛擬、雲端及混合式環境的完整防護

虛擬化已徹底改變了資料中心的樣貌，現在，企業正逐步或全面將其工作負載移轉至私有雲或公有雲。若您也打算善用混合式雲端運算的效益，您務必擁有一套能夠保護您所有伺服器的資安防護，不論實體、虛擬或雲端伺服器。

不僅如此，您的資安防護還不能影響主機效能和虛擬機器 (VM) 密度，或者阻礙虛擬化和雲端運算實現其投資報酬率 (ROI)。趨勢科技 Deep Security™ 在單一解決方案當中提供了完整的資安防護，而且專為虛擬化和雲端環境而打造，因此不會造成資安漏洞、亦不影響效能。

防範資料外洩和業務中斷

Deep Security 提供了軟體、Amazon Web Services (AWS) 或 Microsoft® Azure™ Marketplace 虛擬裝置，以及服務等三種選擇，專為防範資料中心和雲端工作負載的資料外洩和業務中斷而設計。Deep Security 能協助您達成法規遵循要求，經濟而有效率地防堵整個混合式雲端環境的資安漏洞。

從單一儀表板管理多重資安防護

Deep Security 採用惡意程式防護、預判式機器學習、網站信譽評等、防火牆、入侵防護、一致性監控、應用程式控管以及記錄檔檢查等整合式模組，來確保實體、虛擬及雲端環境伺服器、應用程式及資料的安全。 Deep Security 可採用單一多功能代理程式的形式來部署至所有環境，並透過單一儀表板來管理所有功能，簡化資安作業。您可使用趨勢科技 Control Manager 當作儀表板，或者使用第三方廠商的管理系統，如：VMware vRealize Operations、Splunk、HP ArcSight 或是 IBM QRadar。

藉由密切整合將資安政策延伸至雲端環境

Deep Security 能與主流雲端平台密切整合，包括：AWS、Azure 以及 VMware® 工作負載，讓您將資料中心內的資安政策延伸至雲端工作負載。Deep Security 藉由各種專為橫跨不同環境而最佳化的功能，讓企業和服務供應商能夠為其客戶提供差異化且分租共用的安全雲端環境。

企業關鍵問題

虛擬桌面防護

既可維持效能與系統整合率，又能提供完整的防護讓 VDI 環境獲得專為其設計的最大保護。

虛擬修補

防堵漏洞，不讓漏洞遭到攻擊，消除緊急修補、頻繁修補更新部署以及系統停機所帶來的昂貴代價與營運困擾。

法規遵循

證明確實遵守各種法規要求，包括：PCI DSS、HIPAA、NIST、SSAE 16 等等。

> “Deep Security 也讓我們淘汰掉伺服器上安裝的另一套防毒軟體... 這套軟體占用了大量記憶體，而且在執行掃瞄時會消耗大量 CPU 資源。使用 Deep Security 之後這些問題都應刃而解。”

Blaine Isbelle
加州大學柏克萊分校資訊服務科技
系統管理員

值得信賴的混合雲防護

虛擬化防護

Deep Security 能保護虛擬桌面和伺服器，防範零時差惡意程式，包括勒索病毒和網路攻擊，並且盡可能減少資源利用效率不佳或緊急修補所帶來的營運衝擊。

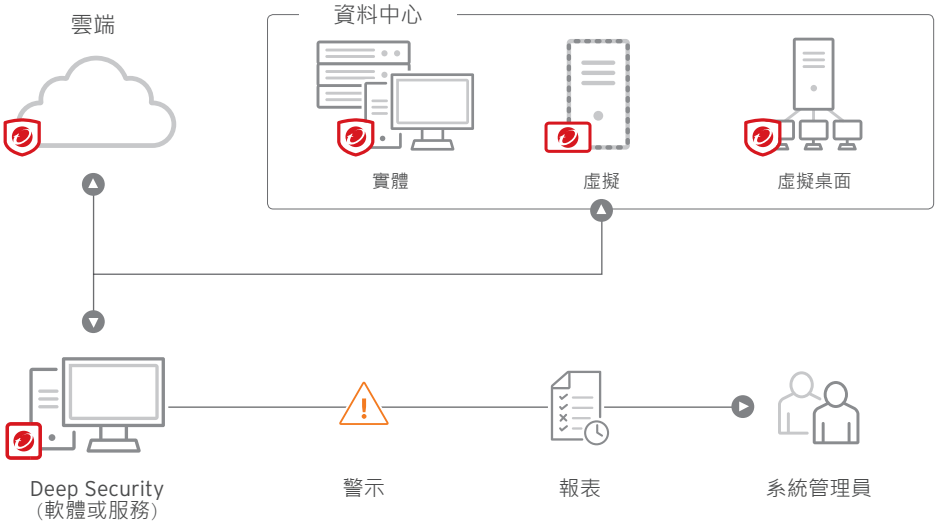
雲端防護

Deep Security 能讓服務供應商和現代化資料中心管理員提供一個安全的分租共用雲端環境，將資安政策延伸至雲端工作負載，透過一致且情境感應的政策來集中管理。

整合式伺服器防護

Deep Security 將所有伺服器防護功能整合至單一、完整、整合且彈性的平台，讓實體、虛擬和容器環境都能享有最大防護。

Hybrid Cloud Security
混合雲防護



主要優勢

有效且高效率

- 提升資源利用效率與管理，比採用傳統惡意程式防護享有更高的虛擬機器 (VM) 密度。
- 透過單一、容易管理的多功能防護代理程式，提供彈性和縱深防禦能力。
- 藉由虛擬化監管程式 (Hypervisor) 層次的非重複掃瞄，提供無可匹敵的效能。
- 與主流雲端平台整合，如：AWS、Microsoft Azure 和 VMware Cloud，讓企業透過一致且情境感應的政策來集中管理實體、虛擬和雲端伺服器。
- 讓服務供應商為客戶提供一個安全的公有雲，藉由分租共用的架構與其他用戶隔離。
- 提供自動擴充、公用運算與自助式服務，支援採用軟體定義資料中心的靈活企業。
- 善用 Deep Security 與 VMware 的密切整合，自動偵測新的虛擬機器並套用情境感應的防護政策，讓資料中心和雲端享有一致的防護。
- 與最新版的 VMware vSphere 和 NSX™ 整合。Deep Security 可透過自動跟隨虛擬機器移動的資安政策和防護，讓微分段發揮更大效益。

盡可能降低營運成本

- 採用集中管理的單一多功能軟體代理程式或虛擬裝置來消除部署多重軟體用戶端的成本。
- 與趨勢科技、VMware 以及 VMware vRealize Operations、Splunk、HP ArcSight、IBM QRadar 等系統的管理主控台整合，降低複雜性。
- 利用惡意程式掃瞄與入侵防護來保護 Docker 主機和容器。
- 將重複性與耗費資源的資安工作自動化，減少因誤判而產生的警示，建立一套資安事件應變流程，進而降低管理成本。
- 利用雲端事件白名單與預先信賴的事件，大幅降低檔案一致性監控的複雜性。
- 偵測漏洞與軟體，透過建議掃瞄來偵測變更並防範漏洞。
- 採用更輕量化、更彈性的智慧型代理程式來減輕部署負擔，有效分配資料中心和雲端的資源，進而提升營運效率。
- 讓資安配合您的政策需求，減少特定資安防護所必須分配到的資源。
- 集中管理所有趨勢科技防護產品，簡化系統管理。集中產生各項資安控管報表，減少產生個別產品報表的麻煩。

避免資料外洩和業務中斷

- 避免不明的應用程式在您最關鍵的伺服器上執行。
- 以最小的效能負荷，即時偵測並移除虛擬伺服器上的惡意程式。
- 藉由多平台應用程式控管，偵測並攔截未經授權的軟體。
- 防堵網站及企業應用程式與作業系統的已知和未知漏洞。
- 利用沙盒模擬分析提供進階威脅偵測與可疑物件防範。
- 當偵測到可疑或惡意活動時發送警示通知並觸發主動防範措施。
- 持續追蹤網站信譽，藉由趨勢科技全球網域信譽評等資料庫的網站信譽情報來防止使用者瀏覽已遭感染的網站。
- 利用趨勢科技全球網域信譽評等資料庫的整合威脅情報來偵測並攔截殭屍網路與針對性攻擊的幕後操縱 (C&C) 通訊。

實現符合成本效益的法規遵循

- 採用單一、整合又符合經濟效益的解決方案來達成重大法規遵循要求，例如：PCI DSS 以及 HIPAA、SSAE 16 等等。
- 提供詳細記載已防止的攻擊與法規遵循狀態的稽核報表。
- 減少稽核的準備時間與人力。
- 支援內部遵規計劃，提升內部網路活動的掌握度。
- 採用通過 Common Criteria EAL 認證的技術。

Deep Security 功能

利用行為監控和預判式機器學習來防範惡意程式

- 與 VMware vShield Endpoint API 整合，保護 VMware 虛擬機器，防範病毒、間諜程式、木馬程式、勒索病毒，以及其他惡意程式。
- 提供一個惡意程式防護代理程式來將防護延伸至實體、虛擬及雲端伺服器，涵蓋 AWS、Microsoft 及 VMware 環境。
- 採用無代理程式的 VMware ESX 層次快取來避免重複掃瞄，進而提升效能。
- 妥善安排資安作業以避免傳統資安防護在執行全系統掃瞄與病毒碼更新時經常發生的防毒風暴。
- 將惡意程式與關鍵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。
- 採用進階機器學習技術來交叉關聯威脅資訊，並且執行深度的檔案分析以偵測新興的未知資安風險。
- 偵測可疑活動或未經授權的變更，並藉由行為監控來加以隔離並迅速復原。
- 藉由沙盒模擬分析來發掘及分析可疑物件。
- 與趨勢科技 Smart Protection Network™ 全球威脅情報網整合，藉由網站信譽評等來強化伺服器與虛擬桌面防護。

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、資安事件、系統管理事件等等，支援 100 多種記錄檔格式。
- 徹底發掘隱藏在多筆記錄內的重要資安事件，達成法規要求 (PCI DSS 第 10.6 條)。
- 將事件傳送至 SIEM 系統或中央記錄伺服器，以便進行關聯分析、報表與歸檔。

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、違反安全政策的情形、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，防止漏洞遭到重複利用，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，達成法規要求 (PCI DSS 第 6.6 條)。
- 防止 SQL 資料隱碼攻擊 (SQL injection)、跨網站腳本攻擊 (cross-site scripting)，以及其他網站應用程式漏洞。
- 防範所有主流作業系統與 100 多種應用程式的漏洞，例如：資料庫、網站、電子郵件、FTP 等伺服器。
- 加強掌握與監控所有會存取網路的應用程式，內含規則可在系統層級防止有害的軟體執行。

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，提供遵規與稽核報表，這對公有雲部署環境尤其重要。

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 (hypervisor) 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。

多平台應用程式控管

- 自動偵測並攔截 Windows 和 Linux 伺服器上未經授權的軟體。
- 掃瞄電腦上所安裝的應用程式。
- 在清查過應用程式清單之後將系統狀態鎖定，自動防止新的應用程式執行，無須建立白名單。
- 與開發營運 (DevOps) 環境整合，支援應用程式清單持續更新，透過 API 來持續控管應用程式。

架構

Deep Security 虛擬裝置。自動在背後強制貫徹 VMware vSphere 虛擬機器防護政策。在 VMware NSX 環境下，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。此外也可採用混搭模式，利用一台虛擬裝置來提供無代理程式的惡意程式防護和一致性監控，另外再搭配一個代理程式來提供入侵防護、應用程式控管、防火牆、網站信譽評等以及記錄檔檢查。

Deep Security 代理程式。這個部署在受保護的伺服器或虛擬機器上的小巧軟體元件，可強制貫徹資料中心的防護政策 (應用程式控管、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。這個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，提供精細的控管。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，並且讓個別承租戶的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。

Deep Security Scanner 是一個與 SAP 系統整合並為其提供防護的模組，可經由 NetWeaver Virus Scan Interface 整合。

SAP Partner

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互通。

部署與整合

利用現有的 IT 和資安投資快速完成部署

- 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、AWS OpsWorks、Microsoft System Center Configuration Manager (SCCM)、Novell ZENworks 以及 Symantec Deployment Solution。
- 提供詳細的伺服器層級安全事件，並可透過各種不同整合選項傳送至 SIEM 系統，如：HP ArcSight、 Intellitactics、IBM Qradar、NetIQ、RSA Envision、Q1Labs、Loglogic、Splunk、Sumologic 以及其他系統。
- 可與企業目錄服務整合，如：Microsoft Active Directory。

Deep Security 採用了靈活的持續創新、開發方法。我們引以自豪的「功能更新版本」採漸進方式陸續推出新的功能，直到下一個重大版本發表為止。這樣的作法是為了讓您不須等到下一次重大版本更新，就能彈性地逐漸享有您所要的功能。

	Deep Security 版本		
防護工具及功能	10.0	10.1 功能更新版本*	10.2 功能更新版本*
應用程式控管	√ Linux	√ + Windows	√
- 全域黑名單			√
- Windows 信賴更新			√
- 事件彙整			√
入侵防護	√	√	√
惡意程式防護	√	√	√
- 行為監控	√	√	√
- 機器學習			√
網站信譽評等	√	√	√
記錄檔檢查	√	√	√
一致性監控	√	√	√
Docker 容器支援	√	√	√
Windows Server 2016	√		√
Deep Security Manager SQL 2016 支援			√
PostgreSQL 支援		√(單一租戶)	√(分租共用與 Multi-AZ 的環境)
零衝擊網路驅動程式安裝		√	√
透過 SAML 2.0 提供單一簽入		√	√
產品內建新聞摘要接收功能		√	√
TippingPoint 與 Deep Security (IPS) 規則對應			√

*在下次 Deep Security 重大版本推出之後，「功能更新版本」將繼續提供六個月。

系統需求

Microsoft® Windows®

- Windows XP、Vista、7、8、8.1、10 (32/64 位元)
- Windows Server 2003 (32/64 位元)
- Windows Server 2008 (32/64 位元)、2008 R2、2012、2012 R2、2012 Server Core (64 位元)、2016 (64 位元)、2016 Server Core (64 位元)
- XP Embedded (32/64 位元)[1]

Linux[2]

- Red Hat® Enterprise 5、6、7 (32/64 位元)[3]
- SUSE® Enterprise 10、11、12 (32/64 位元)[3]
- CentOS 5、6、7 (32/64 位元)[5]
- Ubuntu 12、14、16 (64 位元，僅限 LTS 版本)[4、5]
- Oracle Linux 5、6、7 (32/64 位元)[4、5]
- CloudLinux 5、6、7 (32/64 位元)[2、4]
- Amazon Linux (32/64 位元)[4、5]
- Debian 6、7 (64 位元)[2、4]

Oracle Solaris™[6、7]

- OS：10、11 (64 位元 SPARC)、10、11 (64 位元 x86)[7、8]
- Oracle Exadata Database Machine、Oracle Exalogic Elastic Cloud 及 SPARC Super Cluster (透過支援的 Solaris 作業系統)

UNIX[6]

- AIX 5.3、6.1、7.1 (限 IBM Power Systems)[7、8]
- HP-UX 11i v3 (11.31)[7、9]

虛擬平台

- VMware® vSphere：5.5/6.0、View 4.5/5.0/5.1、ESX 5.5、6.2.X、6.5、NSX 6.2.X、6.3
- Citrix®：XenServer[11]
- Microsoft®：HyperV[11]

1 由於 Windows XP Embedded 可以客製化，因此，客戶必須確認 Deep Security 代理程式運作時所必要的服務和連接埠都已啟用，以確保能夠在客戶的環境當中正確運作。
2 可支援的核心版本請參閱說明文件。
3 SAP 防護僅支援 Red Hat 6 (64 位元) 和 SUSE 11 (64 位元) 代理程式端。SAP 防護要能運作，惡意程式防護模組必須在代理程式端啟用。
4 惡意程式防護僅支援隨選掃瞄。
5 可支援版本請參閱最新的版本發表說明。
6 不提供惡意程式防護和網站信譽評等。
7 透過 9.0 代理程式來提供支援。
8 不提供惡意程式防護。
9 只有記錄檔檢查與一致性監控。
10 vCloud Networking and Security 可支援無代理程式的惡意程式防護和一致性監控。
11 僅能透過 Deep Security 代理程式提供防護。

採用 XGen™ 防護為基礎

採用 XGen™ 防護為基礎的 Deep Security 是趨勢科技 Hybrid Cloud Security 混合雲防護解決方案的一環。

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 2+
- EMC VSPEX 認證
- 與 HP 在業務上合作
- Microsoft Active Protections Program 會員
- 微軟認證合作夥伴
- NetApp FlexPod 認證
- 與 Oracle 合作
- PCI Suitability Testing for HIPS 認證 (NSS Labs)
- SAP 認證 (NW-VSI 2.0 與 HANA)
- VCE Vblock 認證
- VMware 虛擬化認證

Securing Your Journey to the Cloud