Trend Micro™

Deep Security™ Software

實體、虛擬、雲端及容器工作負載的執行時期防護

虛擬化已徹底改變了資料中心的樣貌，而現在，企業正逐漸將其工作負載移轉至雲端或容器架構。混合雲環境固然有諸多優點，但卻也帶來了新的風險和威脅。您的企業必須落實法規遵循，同時確保所有工作負載的安全，包括：實體伺服器、虛擬、雲端以及容器。

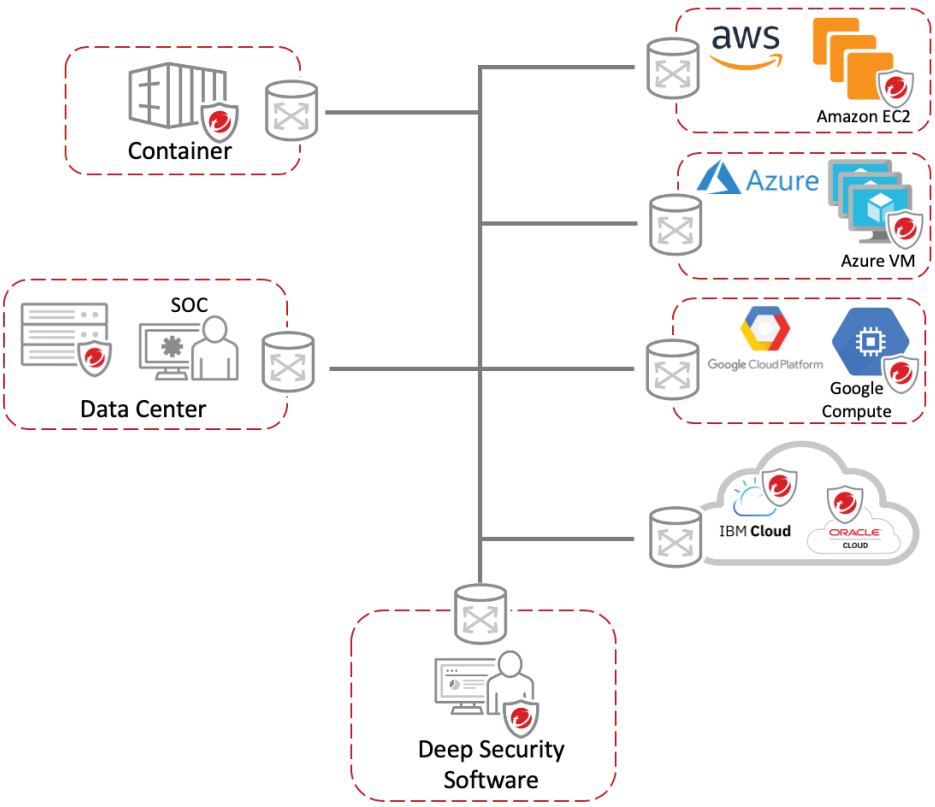
Trend Micro™ Deep Security™ Software 在單一解決方案當中提供了全方位的防護，專為虛擬、雲端及容器環境而打造。Deep Security 不論面對何種工作負載都能提供一致防護，同時更提供了一套豐富完整的應用程式開發介面 (API) 來讓您將防護自動化，避免干擾您的團隊運作

自動化

資安程式碼 (Security as Code) 讓您的 DevOps 團隊將防護融入軟體建構流程當中，如此一來，您的軟體就能頻繁地推陳出新。經由內建的自動化，包括：自動搜尋與部署、快速範本，以及我們的 Automation Center，確保您的環境安全，迅速達成法規要求

彈性

讓開發人員能自由選擇，廣泛支援各種平台的資安防護，能涵蓋混合雲、多重雲端、多重服務 環境以及任何應用程式供應模式。



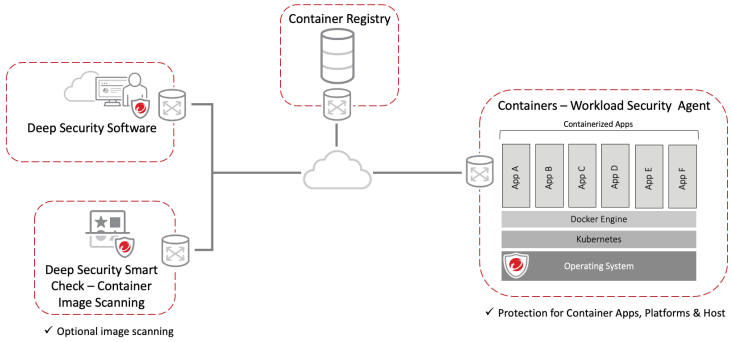
企業關鍵問題

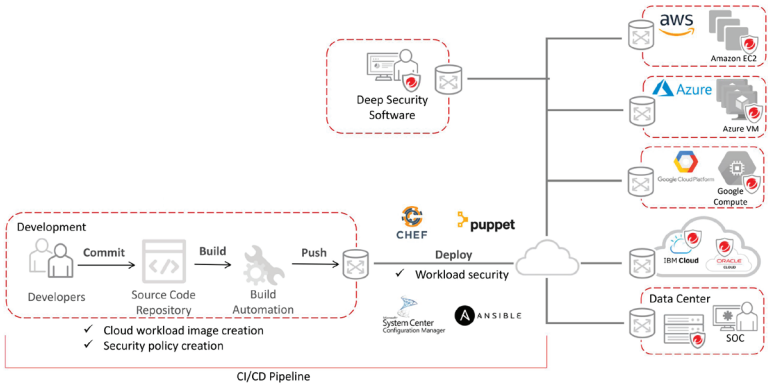
- **自動化防護**
  透過涵蓋各種混合環境 (如資料中心和雲端) 的自動化防護政策，讓您在移轉或建立新的工作負載時能節省時間和資源。
- **全方位的防護**
  藉由單一代理程式和平台來部署並整合實體、虛擬、多重雲端以及容器環境的資安防護。
- **適合 CI/CD 流程的防護**
  提供 API 優先的開發人員導向工具，協助您將資安控管落實到 DevOps 流程當中。
- **加速法規遵循**
  證明確實遵守各種法規要求，包括：GDPR、PCI DSS、HIPAA、NIST、FedRAMP 等等。

值得信賴的混合雲防護

涵蓋完整生命週期的容器防護

Deep Security 提供進階的執行時期容器防護。其多層式的防護能防範針對主機、容器平台 (Docker®)、協調平台 (Kubernetes®)、容器本身，甚至是針對容器化應用程式的攻擊。Deep Security 的設計包含了豐富完整的 API，可讓 IT 資安人員藉由自動化流程來保護容器，達成重要的資安控管。DevOps 可利用資安程式碼將防護融入應用程式開發流程當中，減少在快速變遷或演變的基礎架構當中導入資安防護的阻力。Deep Security 的容器映像掃描功能可讓您在建構流程當中搜尋容器映像內的漏洞、惡意程式、機密以及法規遵循問題，與執行時期的容器防護相輔相成。



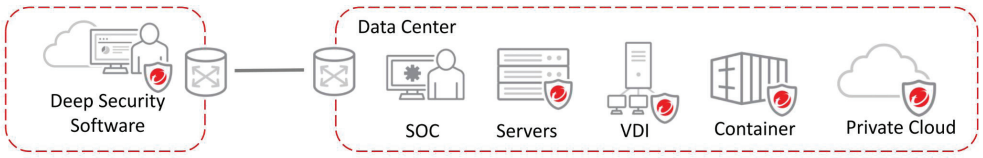


自動化雲端防護

Deep Security 能自動保護雲端工作負載，自動偵測各家雲端廠商的工作負載，包括：AWS、Microsoft® Azure™、Google Cloud™ 等等。Deep Security 的單一管理主控台能統一掌握所有工作負載與自動化防護的狀況，在多重雲端環境能享有一致且隨環境而調整的防護政策。此外，更透過部署腳本與 RESTful API 讓資安防護與您現有的工具整合，實現自動化的防護部署、政策管理、運作狀況檢查、遵規報表等等。

虛擬化與資料中心防護

Deep Security 為實體與虛擬伺服器帶來了進階防護。Deep Security 透過自動化的政策管理，以及與 VMware NSX-V® 和 VMware NSX-T™ 虛擬化監管程式 (hypervisor) 整合的無代理程式防護，讓跨越多重環境的防護部署與管理變得輕鬆容易。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、虛擬加密貨幣挖礦攻擊以及網路攻擊，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。



以全球威脅研究為後盾的資安防護

我們遍布全球的 15 個研究中心與 450 名內部研究人員所組成的情報網，隨時掌握著全球威脅情勢的脈動。我們專精雲端與雲端原生應用程式的專家團隊，將其豐富的知識注入我們的產品當中，防範當前及未來的威脅。

布下天羅地網

我們隨時都在不斷分析、發掘新的惡意程式、勒索病毒、惡意網址、幕後操縱(C&C) 通訊點，以及駭客攻擊可能使用到的網域。

此外，我們也藉由 Zero Day Initiative™ (ZDI) 這個全球規模最大的漏洞懸賞計畫， 不斷廣泛蒐集、揭露各種平台的最新漏洞。

主要優勢

進階威脅防護

- 提供進階的資安控管來保護您的關鍵伺服器與應用程式，包括：入侵防護 (IPS)、一致性監控、機器學習、應用程式控管等等。
- 即時偵測及攔截威脅，幾乎不影響效能。
- 藉由多平台應用程式控管，偵測並防止未經授權的軟體執行。
- 利用 IPS 來防堵網站、企業應用程式及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。
- 利用 IPS 所提供的虛擬修補來保護已終止支援的系統，確保老舊系統的安全，防範目前及未來的威脅。
- 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。
- 偵測及攔截殭屍網路與針對性攻擊的 C&C 通訊。
- 以趨勢科技領先市場的研究為後盾，採用趨勢科技 Smart Protection Network™ 全球威脅情報網的最新情報來防範最新威脅庫的網站信譽情報來防止使用者瀏覽已遭感染的網站。
- 偵測及攔截殭屍網路與針對性攻擊的 C&C 通訊。
- 以趨勢科技領先市場的研究為後盾，採用趨勢科技 Smart Protection Network™ 全球威脅情報網的最新情報來防範最新威脅。

支援並強化事件回應團隊

- 藉由端點偵測及回應 (EDR) 功能來提供事件應變支援， 如：監控攻擊指標、攔截可疑應用程式與執行程序。
- 將 Deep Security 整合至您的資安事件管理 (SIEM) 系統來分 析監測資料以追蹤進階威脅、掃描入侵指標 (IoC)，並與資安 自動化協同及回應 (SOAR) 工具整合來協助矯正與協調作業 的進行。
- 善用趨勢科技的威脅專家來補強您內部團隊的不足，經由 Trend Micro™ Managed XDR. 服務提供您完善的威脅監 控、偵測及分析。這項 7 天 24 小時全天候託管式偵測及回 應 (MDR) 服務，能與其他趨勢科技電子郵件、端點、伺服器/雲端工作負載以及網路等解決方案結合，提供您交叉關 聯的偵測以及整合式調查與回應。

專為混合雲設計的整合式防護

- 藉由雲端及資料中心連動功能來自動發掘您混合雲環境當中執行的工作負載，讓您全面掌握並自動管理政策。
- 消除部署多套單一功能解決方案的成本，透過輕量化的單一代理程式與管理主控台，讓實體、 虛擬、雲端及容器環境皆享有一致的防護。
- 讓您的容器環境在各環節上都能確保安全，包括：主機、容器平台 (Docker)、協調平台 (Kubernetes)、容器本身，以及容器化應用程式。
  - 採用相同的進階主機控管來保護您的容器主機，不論是實體、虛擬機器 (VM) 或雲端工作負載。
  - 透過一致性監控和記錄檔檢查功能來監控 Docker 和 Kubernetes 物件是否出現任何遭到變更或攻擊的跡象。
  - 採用容器漏洞防護 (藉由 IPS)、即時惡意程式防護，以及容器橫向網路流量檢查，來保護執行時期的容器。
- 採用 Trend Micro Cloud One™ – Container Security 的進階建構時期映象與登錄掃描在流程的早期即加入資安防護，再搭配 Deep Security 的執行時期防護，就能保障容器完整生命週期的安全。
- 藉由趨勢科技與 AWS、Azure 及 Google Cloud 等主流雲端廠商的密切整合提供全面的掌握與防護來完整涵蓋多重雲端環境。
- 讓服務供應商能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。
- 進一步延伸軟體定義資料中心微分段 (Microsegmentation) 的效益，透過 Deep Security 與 NSX-V 的整合自動偵測並套用隨環境感應的政策。

自動化與簡化資安防護

- 透過 Deep Security REST API 將資安部署、政策管理、狀況檢查以及法規遵循報表自動化。
- 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。
- 讓資安配合您的政策需求，減少個別資安防護所需配置的資源。
- 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，減少不同產品各自產生報表的麻煩。
- 串連您的防護與您現有的資安及 DevOps 工具，與主流的 SIEM、防護管理、協調、監控、流程以及 IT 服務管理工具整合。

實現符合成本效益的法規遵循

- 透過單一整合又符合成本效益的解決方案，達成重要法規要求，如：通用資料保護法 (GDPR)、支付卡產業資料安全標準 (PCI DSS)、健康保險可攜性與責任法案 (HIPAA) 等等。
- 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可視性。
- 協助整合各種工具，藉由強化的檔案一致性監控功能來達成法規遵循要求。
- 採用通過 Common Criteria EAL 2 和 FIPS 140-2 認證的技術。
- 利用 Container Security 的建構時期容器映象與登錄掃描來落實遵規政策，讓開發流程強制符合法規要求。

> 「擁有像趨勢科技這樣能隨時掌握現代化技術與進階威脅的資安夥伴，讓我們 相信即使是架構發生轉變， 我們的工作負載仍隨時受到妥善防護。」
>
> Jason Cradit
> 資深技術總監
> TRC

系統需求 (管理程式、虛擬裝置、代理程式)

- Deep Security 提供了軟體的購買形式， 可從 AWS 或 Azure 市集購買。詳細的系統需求請參閱以下網址：**https://help.deepsecurity.trendmicro.com/20_0/on-premise/system-requirements.html**
- 軟體服務 (SaaS) 形式：Trend Micro Cloud One™ – Workload Security 防護服務提供與 Deep Security 幾乎完全相同的功能，由趨勢科技負責在雲端內代管，換句話說就是吃重的工作都由我們幫您搞定。我們會負責管理產品及核心的定期更新， 安裝並維護防護相關的資料庫，並且管理其主控台。我們的雲端防護能快速安裝並將雲端執行個體的防護作業自動化及簡化。如需更多資訊，請參閱我們的 Workload Security 網頁

支援的平台 (代理程式)

- 由於趨勢科技可支援的作業系統與版本隨時都在增加，包括：Microsoft® Windows®、 Linux®、Solaris™、AIX® 以及 Docker 容器，完整支援清單請參閱以下網址：https://help.deepsecurity.trendmicro.com/20_0/on-premise/agent-compatibility.html

Deep Security 偵測及防護功能

網路防護工具可偵測及攔截網路攻擊，並且防護含有漏洞的應用程式和伺服器

- **主機入侵防護 (IPS)：**
  利用 IPS 規則來偵測及攔截經由網路攻擊熱門應用程式和作業系統已知漏洞的行為。
- **防火牆：**
  主機防火牆能透過狀態感應的流量檢查來保護網路上的端點。
- **漏洞掃描：**
  掃描作業系統與應用程式可經由網路攻擊的已知漏洞。

系統防護工具可鎖定系統並偵測可疑活動

- **應用程式控管：**
  防止任何非在已知良性應用程式或 DLL 清單中的任何執行檔與腳本在系統上安裝或執行。
- **記錄檔檢查：**
  偵測及警示系統正在發生的非計劃性變更、入侵或進階惡意程式攻擊 (包括勒索病毒)。
- **檔案一致性監控：**
  監控檔案、程式庫、服務等等是否出現變更。為了監控組態設定是否遭到變更，會先建立一個代表安全組態的基準狀態。當這樣 的狀態遭到改變時，就會產生詳細的記錄檔，並且發出警示來通知相關人員。

惡意程式防護可攔截惡意程式與針對性攻擊

- **惡意程式防護：**
  I. 檔案信譽評等—利用我們的惡意程式特徵資料來攔截已知不良的檔案。
  II. 變種防護—利用先前已知惡意程式的片段與偵測演算法來尋找隱晦、變形、變種的惡意程式。
- **行為分析：**
  將未知物件載入執行並觀察其在作業系統、應用程式與腳本中的行為以及相關的互動是否可疑，進而決定是否加以攔截。
- **SAP Scanner*：**
  透過 SAP Virus Scan Interface (VSI) 來為 Netweaver 提供惡意程式掃描。
- **機器學習：**
  利用機器學習演算法來分析未知檔案與零時差威脅，進而判斷是否為惡性。
- **網站信譽評等：**
  攔截已知不良的網址與網站。
- **沙盒模擬分析：**
  將可疑物件送交 Trend Micro™ Deep Discovery™ 網路沙盒模擬分析裝置進行分析，在模擬環境觸發並詳細分析其行為以判斷是否為惡性。接著 Deep Security 會收到確認與快速回應更新，方便採取適當的後續行動。

SAP® Certified
Integration with SAP NetWeaver®

量身訂做的雲端內防護

是專為主流雲端廠商的基礎架構而最佳化，並支援最常見的作業系統：

Linux | Windows | SUSE | redhat | CentOS | ubuntu

此外也相容於各種組態設定、事件管理以及協調工具：

CHEF | puppet labs | OpsWorks | SALTSTACK | splunk> phantom | sumologic | ANSIBLE

SWIMLANE | now | DEMISTO

*SAP Scanner 需要的一些特殊功能必須另外購買，不包含在 Deep Security Software 授權當中。

雲端服務廠商認證 (CSP)

趨勢科技的雲端服務廠商 (CSP) 合作夥伴方案是一項針對全球 CSP 設計的認證計劃，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。

Deep Security 代理程式

這個部署在受保護的伺服器或虛擬機器 (VM) 上的小巧軟體元件，可強制貫徹運算環境的防護政策 (應用程式控管、惡意程式防護、IPS、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®、Ansible、Microsoft SCCM 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 掃描、事件標籤，甚至事件導向工作等作業自動化功能，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。

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 (IPS)、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 IPS、應用程式控管、防火牆、網站信譽評等以及記錄檔檢查。

滿足雲端需求的彈性定價

- 隨時保護著全球數千家客戶、數百萬台伺服器。
- 經由 AWS Marketplace 購買及採購，或者將您自己的授權攜帶至 Azure Marketplace。
- 符合成本效益，隨用量付費：

AMAZON EC2® 執行個體大小	MICROSOFT AZURE 虛擬機器	每小時費用 (美元)
Micro、Small、Medium	1 核心：A0、A1、D1	$0.01
Large	2 核心：A2、D2、D11、G1	$0.03
XLarge (含) 以上	4 核心或更多：A3-A11、D3-D4、D12- D14、G2-G5、D3、D4、D12-D14、G2-G5	$0.06

Deep Security 是 Trend Micro Hybrid Cloud Security 混合雲防護解決方案的一環，該解決方案還包括了 Trend Micro Cloud One™ 這套專為在雲端開發應用程式的企業設計的防護服務平台，包括以下服務：

- **Trend Micro Cloud One™ – Workload Security：**
  實體、虛擬、雲端及容器工作負載的執行時期防護
- **Trend Micro Cloud One™ – Container Security：**
  建構流程中的容器映像掃描
- **Trend Micro Cloud One™ – File Storage Security：**
  雲端檔案及物件儲存服務防護
- **Trend Micro Cloud One™ – Application Security：**
  無伺服器 (Serverless) 功能、API 及應用程式防護
- **Trend Micro Cloud One™ – Network Security：**
  雲端網路層 IPS 防護
- **Trend Micro Cloud One™ – Conformity：**
  雲端資安與法規遵循狀況管理

ZERO DAY INITIATIVE

趨勢科技 ZDI 在 2020 年揭露了全球 60% 的漏洞。這正是我們的虛擬修補速度無人能出其右的原因。

aws

Google Cloud

Azure

vmware

主要認證與策略聯盟

- AWS 進階技術合作夥伴
- AWS Container Competency 合作夥伴
- Common Criteria EAL 2+
- 美國聯邦資訊處理標準 FIPS 140-2 認證
- 與 HP 在業務上合作
- Microsoft 金級應用程式開發合作夥伴
- Microsoft 認證合作夥伴
- SAP 認證 (NW-VSI 2.0 與 HANA)
- VCE Vblock 認證
- VMware 虛擬化
- VMware Cloud on AWS 合作夥伴
- VMware 全球年度合作夥伴

TREND MICRO™

Securing Your Connected World