Trend Micro™

OFFICESCAN™

趨勢科技 XGen™ 端點防護來自值得信賴的領導品牌

過去，資安威脅情勢一向是黑白分明，您要做將威脅擋掉。但現在，好壞變得更難判斷，而且企業對端點防護也更加重視，也認知到僅靠傳統特徵比對的技巧，無法應付那些經常繞過防禦的勒索病毒和未知威脅。而所謂的「次世代」技術，的確有助於對抗某些威脅，但並非全部，然而在同一台端點裝置上安裝多套惡意程式防護軟體，將導致產品過多且不易整合。更麻煩的是，您的使用者越來越常透過各種不同行動裝置、從各種不同地點連至企業內部，甚至雲端服務。您需要能提供全面保護的端點防護，並且是通過市場考驗並值得信賴的廠商，確保防範所有類型的威脅。

趨勢科技 OfficeScan™ 採用了 XGen™ 技術，在威脅防禦技巧當中融入了高準度機器學習能力，能防止任何使用者活動與端點裝置所帶來的資安漏洞。能隨時自我學習、調整，並自動將威脅情報分享至防禦系統。這套融合式威脅防護採用更有效率的端點資源的架構，因此不論在 CPU 和網路利用率方面都超越競爭對手。

OfficeScan 是我們 Smart Protection Suites 智慧型防護套裝軟體當中很重要的一個元件，此套裝軟體甚至提供了其他閘道與端點防護功能，例如：應用程式控管、入侵防護 (漏洞 防堵)、端點加密、資料外洩防護 (DLP) 等，全都整合在單一產品中。此外還有其他趨勢科技解決方案能夠進一步強化您的防護，藉由端點調查和鑑識分析來防範進階攻擊。當本地端發現新的威脅時，Deep Discovery 可藉由網路沙盒模擬分析特徵資料即時更新，讓端點能夠迅速回應，更快具備防護能力，減少惡意程式散布的機會。這些新型態的威脅防護技術，讓企業維運的資訊掌握、管理與報表變得輕鬆簡單。

您可以全部擁有

- **進階的惡意程式和勒索病毒防護：**保護企業網路上或網路外的端點，防範惡意程式、木馬程式、蠕蟲、間諜程式、勒索病毒，並且隨時調整來因應新出現的未知變種。
- **環環相扣的威脅防禦：**OfficeScan 能與您現行網路上的其他防護產品整合，經由趨勢科技的全球雲端威脅情報，能在偵測到新威脅時提供網路沙盒模擬分析資料快速更新給端點，讓端點更快具備防護能力，減少惡意程式散布的機會。
- **集中的資訊掌握及管理：**當搭配趨勢科技 Control Manager™ 一同部署時，就能從單一主控台來管理多台 OfficeScan 伺服器，完全掌握使用者的狀況。
- **行動安全防護整合：**利用 Control Manager 來整合趨勢科技行動安全防護和 OfficeScan，將所有端點的防護管理和政策部署集中化。行動安全防護內含行動裝置威脅防護、行動應用程式管理、行動裝 置管理 (MDM) 以及資料防護。

防護點

- 實體端點
- 虛擬化端點 (選購)
- Windows PC 和伺服器
- Mac 電腦
- POS 銷售櫃台系統和 ATM 提款機

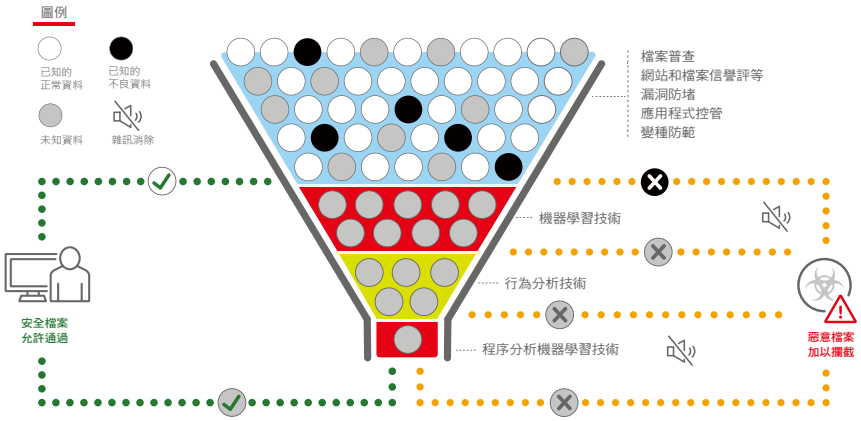
防護點

- 高準度機器學習 (靜態檔案和程序分析)
- 行為分析 (防範腳本、隱碼、勒索病毒、記憶體和瀏覽器攻擊)
- 檔案信譽評等
- 變種防範
- 普查
- 網站信譽評等
- 漏洞防堵 (主機式防火牆、漏洞攻擊防護)
- 幕後操縱 (C&C) 通訊封鎖
- 資料外洩防護 (DLP 模組)
- 裝置控管
- 核對正常檔案
- 沙盒模擬和入侵偵測整合

優勢

最大的端點防護 — XGen

將高準度機器學習與其他偵測技巧融合，提供最廣泛的勒索病毒和進階攻擊防護。



- 層層過濾威脅，採用最有效率的技巧來實現最高的偵測率，同時避免誤判。
- 融合非特徵比對技巧，如：高準度機器學習、行為分析、變種防範、普查、應用程式控管、漏洞攻擊防範、核對正常檔案，再配合檔案信譽評等、網站信譽評等、幕後操縱通訊 (C&C) 攔截等其他技巧。
- 趨勢科技是率先在防護當中融合「高準度」機器學習的廠商，不僅能提供靜態檔案分析，更獨家具備執行程序分析來提高偵測的準確度。
- 在每一層防護當中利用普查和白名單等雜訊消除技巧來降低誤判率。
- 立即將可疑網路活動與可疑檔案的資訊分享給其他防護層，防範後續攻擊。
- 進階勒索病毒防護，在端點上監控可疑的檔案加密活動並予以終止，必要時甚至可復原被加密的檔案。

最小衝擊

降低對使用者的衝擊與管理成本。

- 輕量且最佳化的防護，在適當時機採用適當的偵測技巧，盡可能降低對端點裝置和網路的衝擊。
- 全面集中檢視端點狀態，讓您快速掌握資安風險。
- 自動分享威脅情報給所有防護層，讓整個企業都具備新興威脅防護能力。
- 藉由中繼伺服器 (Edge Relay) 提供企業外的法規遵循與防護，讓員工不必透過 VPN 也能從企業網路外部連上 OfficeScan。
- 可自訂的儀表板，滿足不同管理職務的需求。

通過市場考驗的資安夥伴

趨勢科技一直不斷創新以提供最有效、且最有效率的資安技術。我們總是放眼未來，開發最新的技術來對抗明日瞬息萬變的威脅。

- 累積 25 年以上的資安創新經驗。
- 隨時保護著全球 1.55 億個端點。
- 全球 50 大頂尖企業當中有 45 家都信賴趨勢科技。
- 從 2002 年起即連續入選 **Gartner 端點防護平台神奇象限**「領導者」象限，2016 年更因「完整的願景」而被定位在該象限的最右端。

企業關鍵問題

- 太多惡意程式和勒索病毒繞過資安防禦。
- 需要一套解決方案來防範 PC、 Mac和 VDI 上所有已知和未知的威脅。
- 不同端點防護產品之間無法彼此溝通，拖慢取得防護能力的時間， 又增加管理負擔。
- 從遠端工作的使用者以及透過雲端等新興管道分享資訊所帶來的風險。
- 進階威脅防護和資料防護無法整合造成 IT 效率不彰。

> 「我的第一個目標就是消除之前端點解決方案對我們系統所帶來的沉重負擔。這一點 OfficeScan 做到了。我的第二個目標，就是導入一套真正有效的防護。自從我們換掉先前的解決方案之後，我們看到趨勢科技已阻止了感染的情況。」
>
> **Bruce Jamieson,**
> 加拿大 A&W Food Services
> 網路系統經理

自訂您的端點防護

藉由選購的防護模組來擴充您現有的趨勢科技端點防護，並搭配一些相輔相成的端點解決方案來擴大防護範圍：

資料外洩防護 (DLP) 模組

獲得最大的掌握及管理能力，保護您的機敏資料。

- 保護網路上或離線的機密資料，包括在檔案離開您的網路之前預先加密。
- 防範資料經由雲端空間、外接 USB 隨身碟或行動裝置、藍牙連線以及其他媒體外洩。
- 涵蓋最廣泛的裝置、應用程式和檔案類型。
- 提供更大的掌握與貫徹能力，協助達成法規遵循。

Mac 防護模組

讓您網路上的 Apple Mac 用戶端也能擁有一道防護，避免它們連上惡意網站或散布惡意程式，即使這些惡意程式的攻擊目標並非 Mac OS X 系統。

- 減少接觸網站威脅的機會，包括快速散布且針對 Mac 設計的惡意程式。
- 採用符合 Mac OS X 風格的介面外觀，讓使用者倍感親切。
- 將 Mac 端點也納入集中管理，節省時間和精神。

虛擬桌面基礎架構 (VDI) 模組

讓您將實體桌上型電腦與虛擬桌面的端點防護整合成單一解決方案。

- 自動判斷代理程式是在實體或虛擬端點上執行，並針對所在環境提供最佳的防護和效能。
- 將掃瞄和更新錯開，並利用系統基準白名單和先前掃瞄過的記錄來降低主機資源的消耗。

端點加密

確保資料私密性，將端點上儲存的資料加密，包括：PC、Mac、DVD 和 USB 隨身碟，後兩者非常容易遺失或遭到竊取。趨勢科技 Endpoint Encryption 端點加密可提供您所需的資料防護，包括：全磁碟加密、資料夾與檔案加密、抽取式媒體加密。

- 藉由全磁碟加密軟體來保護儲存中的資料。
- 利用自我加密硬碟讓資料管理自動化。
- 將個別檔案、共用資料夾、抽取式媒體上的資料加密。
- 設定精細的裝置控管與資料管理政策。
- 管理 Microsoft Bitlocker 和 Apple FileVault。

漏洞防護

立即防範您的實體桌上型電腦、筆記型電腦和虛擬桌面遭到零時差威脅攻擊，不論在網路上或離線。採用主機式入侵防護系統（HIPS）的趨勢科技 Vulnerability Protection 能防範已知和未知漏洞，直到修補程式釋出或能夠部署為止。將防護延伸至重要的平台，包括老舊的作業系統（如 Windows XP）。

- 藉由虛擬修補來防堵漏洞，減少暴露在危險中的機會。
- 減少系統復原與緊急修補的停機時間。
- 讓您按照自己的進度和時間表來安排系統修補。
- 發掘資安漏洞並提供顯示 CVE 編號、MS 編號及嚴重性的報表。

端點應用程式控管

提升您的惡意程式與針對性攻擊防禦能力，防止不當及未知的應用程式在企業端點上執行。

- 防止使用者或電腦執行惡意軟體。
- 動態調整政策來降低管理衝擊，提供彈性來配合活躍的使用者環境。
- 鎖住系統，僅允許使用您企業核准的應用程式。
- 利用從數十億個檔案交叉關聯分析出來的威脅資料隨時更新已知正常的應用程式名單。

端點感知

提供具備環境感知能力的端點調查與鑑識分析能力，記錄詳細的系統層級活動並提供報表以方便執行威脅分析，快速評估攻擊的性質和範圍。Deep Discovery 的客製化偵測能力、情報及控管讓您：

- 偵測及分析攻擊您的駭客。
- 立即因應攻擊而調整防護。
- 在資料外洩之前迅速因應。

趨勢科技 Control Manager™

這套防護集中管理主控台，能確保防護管理的一致性，提供完整的掌握與報表，涵蓋趨勢科技多重環環相扣的防護層。此外，還可將掌握及掌控能力延伸至企業內、雲端以及混合式部署環境。集中式管理再配合使用者導向的檢視，能提升防護，降低複雜性，去除多餘重複的防護管理工作。此外，Control Manager 還能讓您取得趨勢科技 Smart Protection Network™ 的威脅情報以便採取行動，該情報網能利用全球威脅情報在雲端提供即時防護，在您接觸到威脅之前預先加以攔截。

OFFICESCAN 系統需求

伺服器最低建議需求

OfficeScan 伺服器作業系統：
- Windows Server 2008 (SP2) 和 2008 R2 (SP2) (x64) Editions
- Windows Storage Server 2008 (x86/x64) 和 Storage Server 2008 R2 (SP1) (x64) Editions
- Windows HPC Server 2008 和 HPC Server 2008 R2 (x64)
- Windows MultiPoint Server 2010 (x64) 和 2012 (x64)
- Windows Server 2012 和 2012 R2 (x64) Editions
- Windows MultiPoint Server 2012 (x64) Editions
- Windows Storage Server 2012 (x64) Editions
- Windows Server 2016 (x64) Editions

OfficeScan 伺服器平台：
處理器：1.86 GHz Intel Core 2 Duo (雙 CPU 核心) 或更高
記憶體：最低 1 GB (建議 2 GB)，至少保留 500 MB 給 OfficeScan 專用 (Windows 2008)
- 最低 2 GB，至少保留 500 MB 給 OfficeScan 專用 (Windows 2010/2011/2012/2016)

磁碟空間：至少 6.5 GB (遠端安裝至少需 7 GB)

OfficeScan 邊界中繼 (Edge Relay) 伺服器平台：
處理器：2 GHz Intel Core 2 Duo (雙 CPU 核心) 或更高 Memory: 4 GB minimum
記憶體：至少 4 GB
磁碟空間：至少 50 GB 作業系統
Windows Server 2012 R2 網路卡：
1. 雙網路卡組態
   - 一張讓企業內網路連上 OfficeScan 伺服器。
   - 一張讓企業外部的 OfficeScan 代理程式連線。
2. 單網路卡組態則藉由不同的連接埠來區隔企業內與企業外連線。

資料庫：
1. SQL Server 2008 R2 Express (或更新版本)
2. SQL Server 2008 R2 (或更新版本)

代理程式最低建議需求

代理程式作業系統：
- Windows XP (SP3) (x86) Editions
- Windows XP (SP2) (x64) (專業版)
- Windows Vista (SP1/SP2) (x86/x64)
- Windows 7 (含或不含 SP1) (x86/x64)
- Windows 8 和 8.1 (x86/x64)
- Windows 10 (32 和 64 位元)
- Windows 10 IoT Embedded
- Windows Server 2003 (SP2) 和 2003 R2 (x86/x64)
- Windows Compute Cluster Server 2003 (主動/被動)
- Windows Storage Server 2003 (SP2) 和 Storage Server 2003 R2 (SP2) (x86/x64)
- Windows Server 2008 (SP2) (x86/x64) 和 2008 R2 (SP1) (x64)
- Windows Storage Server 2008 (SP2) (x86/x64) 和 Storage Server 2008 R2 (x64)
- Windows HPC Server 2008 和 HPC Server 2008 R2 (x86/x64)
- Windows Server 2008/2008 R2 Failover Clusters (主動/被動)
- Windows MultiPoint Server 2010 和 2011 (x64)
- Windows Server 2012 和 2012 R2 (x64)
- Windows Storage Server 2012 和 2012 R2 (x64)
- Windows MultiPoint Server 2012 (x64)
- Windows Server 2012 Failover Clusters (x64)
- Windows Server 2016 (x64)
- Windows XP Embedded Standard (SP1/SP2/SP3) (x86)
- Windows Embedded Standard 2009 (x86)
- Windows Embedded POSReady 2009 (x86), Embedded POSReady 7 (x86/x64)
- Windows 7 Embedded (x86/x64) (SP1)
- Windows 8 和 8.1 Embedded (x86/x64)

代理程式平台：
處理器：300 MHz Intel Pentium 或同等級處理器 (Windows XP、2003、7、8、8.1、10)
- 最低 1.0 GHz (建議 2.0 GHz) Intel Pentium或同等級處理器 (Windows Vista、Windows Embedded POS、Windows 2008 (x86))
- 最低 1.4 GHz (建議 2.0 GHz) Intel Pentium 或同等級處理器 (Windows 2008 (x64)、Windows 2016)

記憶體：最低 256 MB (建議 512 MB)，至少保留 100 MB 給 OfficeScan 專用 (Windows XP、2003、Windows Embedded POSready 2009)
- 最低 512 MB (建議 2.0 GB)，至少保留 100 MB 給 OfficeScan 專用 (Windows 2008、2010、2011、2012)
- 最低 1.0 GB (建議 1.5 GB)，至少保留 100 MB 給 OfficeScan 專用 (Windows Vista)
- 最低 1.0 GB (建議 2.0 GB)，至少保留 100 MB 給 OfficeScan 專用 (Windows 7 (x86)、8 (x86)、8.1 (x86)、Windows Embedded POSReady 7)
- 最低 1.5 GB (建議 2.0 GB)，至少保留 100 MB 給 OfficeScan 專用 (Windows 7 (x64)、8 (x64)、8.1 (x64))

磁碟空間：至少 650 MB

如需更詳細的系統需求請至： docs.trendmicro.com。

> 「像我們這樣遍布全國的網路，能夠透過單一平台來保 護行動和桌上型裝置，不僅 簡化了我們的網路，也讓我們的團隊更有生產力。」
>
> **Greg Bell,**
> IT 總監
> DCI Donor Services

TREND MICRO™

Securing Your Journey to the Cloud