趨勢科技

Apex Central Advanced Edition

集中掌握與監控

在今日精密複雜的威脅情勢當中，進階攻擊會利用多重威脅管道來進入使用者的端點、伺服器、網路、網站及電子郵件。您需要全面掌握各個防護層才能確保企業獲得最佳防護。此外，隨著 IT 逐漸移轉至雲端，您還需要能夠同時管理企業內、雲端及混合雲環境的資安防護。

一致的防護管理能協助您跨越不同防護層及不同部署模式之間的 IT 藩籬。像這樣的集中化管理，能提升掌握、降低複雜性、消除重複性防護管理工作，而這一切都能讓您的企業更安全，讓管理更輕鬆。

這套集中式掌握與監控解決方案提供了單一整合的介面來管理、監控所有的防護層並提供報表，經由 Apex Central™ 軟體服務或企業內部署的趨勢科技 Control Manager™ 來達成。可自訂的儀表板能讓您完全掌握狀況，快速評估當下狀態、發掘威脅，並且回應資安事件。使用者導向的呈現 (經由與 Active Directory 整合) 查看使用者所有端點、裝置的狀況及其電子郵件與網站流量，同時也讓您檢視政策狀態，變更使用者相關的一切設定。

而且，萬一真的爆發疫情，您將能掌握環境的整體狀態，並且追蹤威脅的擴散源頭。只要能對資安事件有更深入的了解，就更能防範事件重複發生。此外，還能直接連上趨勢科技 Threat Connect™ 資料庫來獲得可採取行動的威脅情報，讓您了解惡意程式樣本、作者與散布手法之間的複雜關係。

Apex Central 可支援的趨勢科技產品

- Hybrid Cloud Security **混合雲防護**
- Deep Security
- Network Defense **網路防禦**
- Deep Discovery Inspector
- Deep Discovery Analyzer
- Deep Discovery email Inspector
- User Protection **使用者防護**
- ApexOne endpoint protection
- Worry-Free™ Business Security
- Endpoint Encryption
- Endpoint Application Control
- Endpoint Sensor
- Security for Mac
- Vulnerability Protection
- Data Loss Prevention
- 行動安全防護
- InterScan™ Messaging Security
- ScanMail™
- Hosted Email Security
- Portal Protect
- InterScan™ Web Security
- Cloud App Security

Apex Central™ as a Service 可支援的趨勢科技產品

- Apex One™ as a Service，**包括以下服務：**
  - *Apex One™ as a Service:* Application Control
  - *Apex One™ as a Service:* Vulnerability Protection
  - *Apex One™ as a Service:* DLP (資料外洩防護)
- Apex One™ as a Service
- Apex One™ (Mac) as a Service
- Apex One™ as a Service: Endpoint Sensor
- Apex One™ (Mac) as a Service: Endpoint Sensor

主要優勢

輕鬆掌握企業整體狀況

- 在軟體服務 (Apex Central™ as a Service) 與企業內 (Control Manager) 皆提供相同的功能。
- 持續監控及迅速了解您的防護狀況、發掘威脅，並且回應資安事件，隨時掌握整體環境的最新情況。而且當有威脅真的入侵到您的環境內部時，您還能調查其擴散源頭。
- 直覺式、可自訂的介面，不僅讓您查看所有防護層與使用者的狀況，更能深入您想要尋找的特定資訊。
- 防護儀表板讓資訊一目了然，如此一來，系統管理員就能優先處理重大的威脅、重要的使用者或重要的端點裝置，立即解決最迫切的問題。
- 可自訂的儀表板和報表、自訂查詢以及警示，提供您採取行動所需的資訊以確保安全與法規遵循狀態。
- 能輕鬆融入您的資安營運中心 (SOC)，與主流的 SIEM 解決方案整合。
- 預先定義的報表範本與可自訂的 SQL 報表，協助您達成內部 IT 稽核與外部法規要求。

環環相扣的威脅防禦給您更好的防護

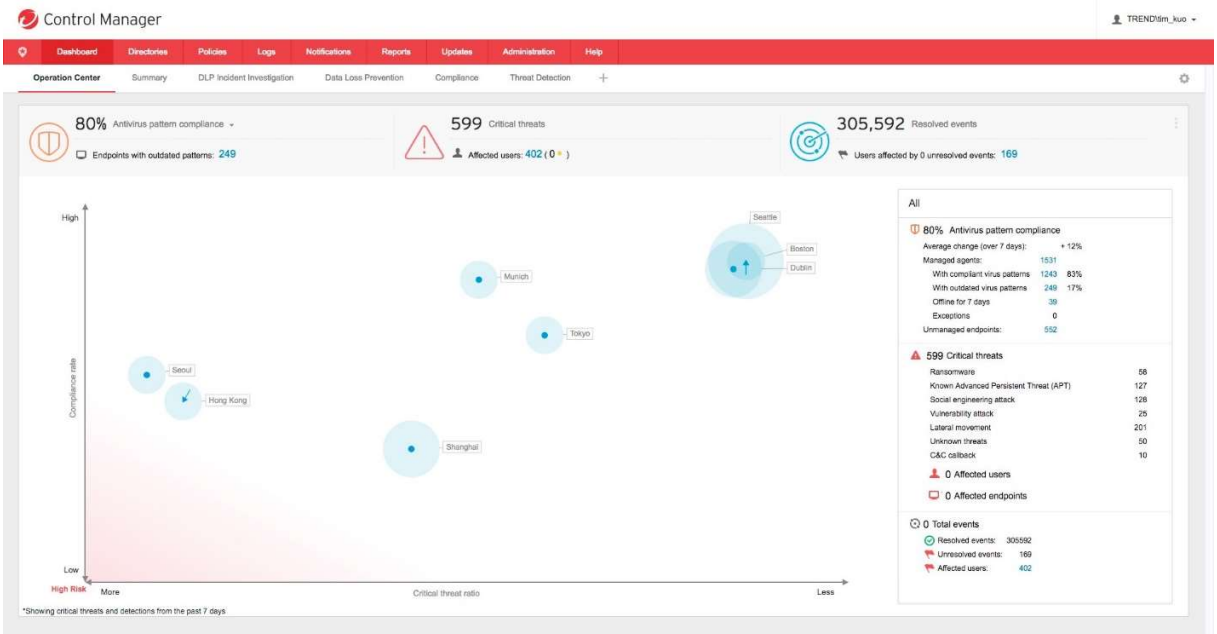
(僅限趨勢科技 Apex Central)

卓越的威脅調查與情報

- 完整的威脅回應及調查能力，讓您追溯並找出某個威脅從何處開始在您的企業內擴散，以及完整的背景資訊、事件時間軸與攻擊範圍，讓您迅速回應駭客入侵。
- 直接連上我們的 Threat Connect™ 資料庫，提供您可採用行動的全球威脅情報。其中包括豐富、交叉關聯的威脅資料，詳細說明威脅的行為特徵 (如網路活動與系統修改) 以及全面性、系統性或產業相關的影響。
- 趨勢科技知識庫能提供矯正及預防的建議。

掌握使用者相關資訊

- 多重層次的掌握能力，不論您的防護是部署在企業內或雲端內， 提供您集中的單一檢視，讓您不需在不同主控台之間來回切換。
- 簡化的防護管理，讓經由單一整合的操作介面來管理端點、伺服器、網路、行動裝置、訊息、協同作業及網站的威脅防護與資料防護。
- 藉由與 Active Directory 整合來簡化儀表板，根據 AD 據點和部門提供交叉關聯資料。
- 使用者導向的檢視讓您輕鬆管理所有裝置的防護，針對個別使用者的任意端點裝置部署政策並檢視其狀態，不論是桌上型電腦或行動裝置。



防護儀表板採用創新的熱區圖 (可根據 Active Directory 的據點和部門資訊) 來顯示對 IT 與資安系統管理員最重要的防護狀況以及重大威脅。

系統需求(最新需求請以官網為準)

伺服器硬體需求
Ô 處理器：最低 2.3 GHz Intel™ Core™ i5 或相容處理器；AMD™ 64 處理器；Intel 64 處理器
Ô **記憶體：至少** 8 GB
Ô 可用硬碟空間：至少 80 GB (SAS 硬碟)

軟體需求
作業系統
Ô Microsoft™ Windows™ Server 2008 Standard/Enterprise Edition 含 SP2
Ô Windows Server 2008 (R2)、Standard/Enterprise/Datacenter Edition 含 SP1
Ô Windows Server 2012 Standard/Datacenter Edition (64 位元)
Ô Windows Server 2012 (R2) Standard/Datacenter Edition (64 位元)
Ô Windows Server 2016 Standard/Datacenter Edition (64 位元)
網頁主控台
Ô 處理器：300 Mhz Intel™ Pentium™ 處理器或同等級處理器
Ô 記憶體：至少 128 MB
Ô 可用硬碟空間：至少 30 MB
Ô 瀏覽器：Microsoft Internet Explorer™ 11、Microsoft Edge™、Google Chrome (註：當使用 Internet Explorer 或 Edge 時，請關閉「相容性檢視」)
Ô 其他：1366 x 768 解析度及 256 色或更高規格的螢幕；Adobe™ Flash™ 8 或更新版本
資料庫軟體
Ô SQL Server 2008 Express 含 SP4
Ô SQL Server 2008 (R2) Standard/Enterprise 含 SP3
Ô SQL Server 2008 Standard/Enterprise 含 SP4
Ô SQL Server 2012 Express 含 SP3
Ô SQL Server 2012 Standard/Enterprise 含 SP3
Ô SQL Server 2014 Express 含 SP2
Ô SQL Server 2014 Standard/Enterprise 含 SP2
Ô SQL Server 2016 Express 含或不含 SP1
Ô SQL Server 2016 Standard/Enterprise 含或不含 SP1
虛擬化支援
Control Manager 可支援其所在作業系統所支援的虛擬平台

主要效益

- 採用創新的熱區圖資安儀表板，更方便掌握防護的狀況。
- 採用中央主控台來簡化資安及資料政策的管理。
- 採用可重複使用的政策範本來管理整個 IT 基礎架構的整合式資料外洩防護，進而提升資料保護。
- 將更新與資安警示整合，再配合環環相扣的威脅防禦在各防護層之間共享資訊，進而降低風險。
- 節省時間、減輕 IT 人員的負擔，降低防護管理成本。

TREND MICRO™

Securing Your Connected World