趨勢科技

Apex One™

來自您信賴的領導品牌- 提供自動化、全面掌握、全方位的端點防護

過去，資安威脅情勢一向是黑白分明，您要做的就是讓好的進來、將不好的濾掉。但現在，好壞變得更難判斷，而且光靠傳統特徵比對的防毒技巧，無法應付那些經常越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，將導致產品過多且無法整合。更麻煩的是，您的使用者越來越常透過各種不同裝置、從各種不同地點連上企業資源，甚至雲端服務。因此，企業需要一套精準、最佳化、環環相扣且來自您信賴品牌的端點防護。

趨勢科技 Apex One™ 融合了各種進階威脅防護技巧來消除資安漏洞，保護使用者的任何活動和端點。能隨時自我學習、調整，並自動將威脅情報分享至整個環境。

這套融合式防護採用更能有效利用端點資源的架構，因此不論在 CPU 和網路利用率方面都超越競爭對手：

- 藉由自動偵測及回應來防範日益多樣化的威脅，包括無檔案式威脅和勒索病毒。
- 透過進階的端點偵測及回應 (EDR) 工具、託管式偵測及回應 (MDR) 服務、強大的 SIEM 整合，以及開放的程式開發介面 (API)，全面掌握、調查並集中檢視網路的整體狀況。
- 透過全方位的輕量化代理程式來實現部署彈性，具備軟體服務 (SaaS) 或企業內部署兩種選擇。

Apex One™ 是我們 **Smart Protection Suites** 當中很重要的一環，此套裝軟體提供了閘道與端點防護功能，例如：應用程式控管、入侵防護 (漏洞防護)、趨勢科技 Endpoint Encryption™、Data Loss Prevention™ (DLP) 等等，全都整合在單一套裝方案當中。此外還有其他趨勢科技解決方案能夠藉由端點調查及回應 (EDR) 來進一步擴充您的調查能力。而這一切現代化威脅防護技術，都能經由集中的掌握、管理與報表，讓您的企業輕鬆擁有。

防護點

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

您可以全部擁有

- **進階惡意程式與勒索病毒防護：**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與進階威脅，如：虛擬加密貨幣挖礦惡意程式和無檔案式惡意程式。
- **偵測及回應能力：**Apex One™ 已內含進階偵測及回應功能。除此之外，還可添購趨勢科技 Endpoint Sensor 調查工具以及託管式偵測及回應 (MDR) 服務。
- **業界最即時的虛擬修補功能：**Apex One™ Vulnerability Protection™ 可利用虛擬化方式修補已知及未知的漏洞，在修補更新釋出或可部署之前，即可防範已知與未知的漏洞。
- **環環相扣的威脅防禦：**Apex One™ 能與您本地端網路上的其他防護產品整合，而且，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。
- **集中掌握及監控：**當搭配趨勢科技 Apex Central™ 一同部署時，就能從單一主控台來管理各種功能，集中掌握及監控所有功能。
- **行動安全防護整合：**利用 Apex Central™ 來整合趨勢科技行動安全防護與 Apex One™，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。
- **企業內部署與服務兩種選擇：**Apex One™ 可部署在您的企業網路內，或採用軟體服務方式部署，兩種部署方式皆提供相同的產品功能。

企業關鍵問題

* 太多惡意程式和勒索病毒越資過安防線，進階威脅不斷躲過執行前靜態檔案偵測。
* 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。
* 針對不斷湧入的警示很難進行交叉關聯分析並判斷能其優先次序。
* 使用者在面對潛在威脅時需要更多自動化分析資訊能力。
* 不同端點防護產品之間無法彼此溝通，既拖慢取得防護能力的時間，又增加管理負擔。
* 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資安風險。
* 很難快速徹底修補端點裝置，因而造成資安上的漏洞。

防護點

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

威脅偵測能力

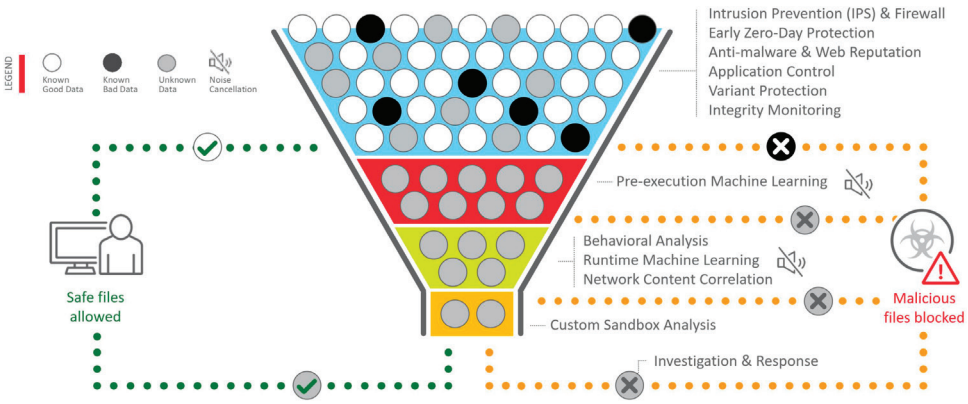
- 高準度機器學習 (執行前靜態檔案偵測和執行中程序分析)
- 行為分析 (防範腳本、隱碼、勒索病毒、記憶體和瀏覽器攻擊)
- 檔案信譽評等
- 變種防護
- 普查
- 網站信譽評等
- 漏洞攻擊防範 (主機防火牆、漏洞攻擊防護)
- 幕後操縱 (C&C) 通訊攔截
- 資料外洩防護
- 裝置控管
- 良性檔案檢查
- 沙盒模擬分析及入侵偵測整合
- 偵測及回應
- 端點加密
- 漏洞防護

看看我們在競爭評比中的表現

https://www.trendmicro.com/en_us/business/technologies/competitive-benchmarks.html

XGen™ 最大防護

- 將高準度機器學習與其他進階偵測技巧融合，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、變種防護、普查、應用程式控管、漏洞攻擊防範、良性檔案檢查，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。
- 趨勢科技率先在防護當中融合「高準度」機器學習，不僅能提供執行前靜態檔案偵測，更獨家具備執行中程序分析來提高偵測的準確度。
- 此外更在每一層防護當中加入普查 (census) 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。

趨勢科技 User Protection 使用者防護解決方案是以 XGen™ 防護為基礎，提供精準、最佳化、環環相扣的防護。

最小衝擊

降低對使用者的衝擊與管理成本。

- Apex One™ as a Service (僅包含在 Smart Protection Suites 當中) 可讓您從我們的雲端服務來部署與管理 Apex One™，並且提供與企業內部署方式完全相同的功能。
- 其輕量且最佳化的代理程式，可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。
- 藉由邊界中繼 (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 Apex One™。
- 可自訂的儀表板，滿足不同管理職務的需求。
- 7 天 24 小時的支援，意味著只要發生問題，趨勢科技都能盡速解決。

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。

- 30 年的資安創新經驗。
- 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 家皆信賴趨勢科技。
- 趨勢科技是 2018 年 Gartner 端點防護平台神奇象限 (Gartner Magic Quadrant for Endpoint Protection Platforms) 報告 21 家廠商當中獲選為「領導者」的三家廠商之一。

點選此處來進一步了解詳情

https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html#_blank"https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html

自訂您的端點防護

Apex One™ 可讓您自由選擇額外的防護與調查功能來擴充您的端點防護。可選擇滿足您企業獨特資安需求的各種進階功能。

> 「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防護，也讓我們的團隊更有生產力。」
>
> **Greg Bell**
> IT 總監
> DCI Donor Services

Vulnerability Protection

Apex One™ 的虛擬修補功能是以世界級的漏洞研究為後盾，能提供業界最即時的漏洞防護，保護各式各樣的端點，包括：銷售櫃台系統 (POS) 和物聯網 (IoT) 裝置，以及作業系統已終止支援 (EOS) 的裝置。

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，不論是否連上網路。趨勢科技 Vulnerability Protection 以及趨勢科技的端點防護功能可將防護延伸至一些關鍵的平台，包括 Microsoft® Windows® XP 之類的老舊系統。

防範進階威脅

- 在修補更新套用之前預先攔截已知及未知的漏洞攻擊。
- 保護不再釋出修補更新的已終止支援或老舊作業系統。
- 針對您的環境自動評估和建議所需的虛擬修補。
- 根據端點所在位置動態調整防護組態。
- 在不影響網路吞吐量、效能以及使用者生產力的情況下保護端點。
- 為端點提供多層式防護，防範不當的網路流量。
- 保護儲存敏感資料的系統，達成法規與企業政策要求。

移除企業營運關鍵流量當中的不良資料

- 套用控管過濾規則來警示/封鎖特定流量，如：即時通訊、媒體串流。
- 利用深層封包檢查來發掘可能傷害應用程式的內容。
- 運用狀態感應的流量檢查，過濾管制的網路流量，確保正常流量順暢。

提供早期防護

- 在修補更新部署之前 (甚至經常在修補更新釋出之前) 提供防護。
- 保護作業系統和常用應用程式，防止已知和未知的攻擊。
- 偵測在非標準連接埠上使用常見通訊協定以躲避偵測的惡意流量。
- 藉由網路漏洞偵測，封鎖可能攻擊裝置漏洞的流量。
- 防止經由網路運作的後門程式滲透企業網路。
- 利用入侵防護特徵規則來防範所有已知的漏洞攻擊。
- 利用客製化過濾規則來攔截使用者定義的參數，保護客製化與老舊的應用程式。

針對現有基礎架構的部署與管理

- 利用簡化的儀表板來提升精細控管的方便性，從管理主控台掌握使用者的狀況。
- 根據 Microsoft 的資安公告編號、CVE 編號或其他重要資訊來安排漏洞評估。
- 將記錄檔與熱門的 SIEM 工具整合。
- 利用 Apex One™ 的單一代理程式和集中掌握與監控來簡化部署與管理。

軟體

防護點

- 端點裝置

威脅防護

- 漏洞攻擊
- 阻斷服務攻擊
- 不當的網路流量
- 網站威脅

功能及效益

- 避免錯過任何修補更新所造成的風險。
- 延長老舊及終止支援作業系統 （如 Windows XP) 的使用年限。
- 透過漸進式的零時差攻擊防護，減少停機復原的時間。
- 讓您按照自己的進度和時間表來安排系統修補。
- 提升資料防護法規遵循狀態來降低潛在的法律風險。
- 加強防火牆防護來保護遠端和行動的企業端點。

Application Control

趨勢科技 Apex One™ Application Control™ 能提升對惡意程式與針對性攻擊的防禦力，防止未知及不當的應用程式在企業端點上執行。這套容易管理的解決方案結合了彈性的動態政策、白名單與黑名單功能，再搭配豐富完整的應用程式目錄，能大幅減少端點裝置遭到攻擊的機會。若需要更完整的威脅資訊以及使用者導向的檢視與政策管理，可透過 Apex Central™ 的集中管理來達成。此外，Apex Central™ 還可將掌握及監控能力延伸至所有企業內、雲端以及混合式部署環境。經由趨勢科技環環相扣的威脅防護，從本地端沙盒模擬分析或趨勢科技 Smart Protection Network™ 取得可採取行動的威脅情報，後者藉由全球威脅情報從雲端提供即時的防護，在威脅到達使用者之前預先加以攔截。

功能及效益

防範惡意程式、針對性攻擊與零時差威脅的強化防護

- 預防因執行了不當或未知的應用程式所帶來的潛在損害 (包括：執行檔、DLL、Windows Store 應用程式、裝置驅動程式、控制台以及其他 PE 執行檔)。
- 藉由全球交叉關聯分析情報網的良性檔案信譽評等資料，提供全球與本地端即時威脅情報。
- 與其他防護層環環相扣，強化威脅資料關聯分析，更有效攔截更多威脅。
- 採用趨勢科技 Smart Protection Network™ 超過 10 億筆以上的良性檔案資料所分析和交叉關聯出來的應用程式資料。
- 可搭配防毒、主機入侵防護、資料外洩防護以及行動安全防護等產品。

簡化管理以提升防護速度

- 利用客製化儀表板與管理主控台提升精細控管的方便性。
- 採用智慧動態政策，以多項信譽評等參數 (如應用程式普遍性、區域性使用頻率及成熟度) 為依據，讓使用者仍可安裝良性的應用程式。
- 藉由使用者導向的檢視、政策管理與記錄檔彙整，針對威脅爆發事件提供更深入的分析資訊。透過 Apex Central™ 來彙整趨勢科技多個防護層的報表。
- 透過趨勢科技的 Certified Safe Software Service 提供應用程式分類並定期更新以簡化管理。

深度的白名單與黑名單，攔截未知及不當的應用程式

- 利用應用程式名稱、檔案路徑、正規表示法 (regular expression) 或憑證來建立基本的應用程式白名單和黑名單。
- 可從趨勢科技定期更新的應用程式目錄當中選取各種預先分類的應用程式名單。
- 藉由可靠的變更來源，確保白名單內的應用程式能夠安裝修補更新，並且讓您藉由更新程式來安裝新的修補更新。
- 可針對內部自行開發或未在名單上的應用程式建立您自己的應用程式白名單與黑名單。
- 提供無可匹敵的應用程式涵蓋度與良性檔案資料。

落實內部 IT 政策，協助降低法律與財務風險

- 針對特定使用者或端點，限制只能使用資料外洩防護 (DLP) 產品可支援的特定應用程式。
- 針對軟體授權蒐集並限制應用程式的使用量。
- 提供系統鎖定功能，防止新的應用程式執行，進一步強化終端使用者系統的安全。

> 「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。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
網路系統經理
A&W Food Services of Canada

Data Loss Prevention (DLP)

趨勢科技 Apex One™ Data Loss Prevention™ (DLP) 將資料外洩防護功能直接整合至您現有的趨勢科技端點解決方案當中，進而降低資料防護的複雜性與成本。讓您迅速輕鬆掌握及監控您的敏感資料，防止資料經由 USB、電子郵件、SaaS 應用程式、網站、行動裝置及雲端儲存外洩。採用內建的區域性及產業相關範本來簡化部署，協助您遵守區域性法規和規範。Apex One™ DLP™ 讓您只需花費傳統企業資料外洩防護解決方案的少許成本和時間就能部署資料防護。

功能及效益

強化資料防護與控管

- 讓 IT 透過精細的裝置控管與資料外洩防護政策來管制 USB 隨身碟、USB 連接的行動裝置、CD/DVD 燒錄機、雲端儲存以及其他可卸除式媒體的使用。
- 利用 DLP for Microsoft® Office 365® 來強制雲端儲存及 SaaS 應用程式使用檔案加密。
- 根據關鍵字、正規表示法 (regular expression) 以及檔案屬性來偵測並回應不當的資料使用行為。
- 透過警示、攔截、軟性阻擋及報表來教育員工認識企業資料使用政策。

支援法規遵循

- 利用內建的遵規範本來簡化法規遵循作業。
- 利用鑑識分析資料擷取與即時報表來加快稽核和強制貫徹。
- 提供區域特定的範本與資料保護選項，協助客戶遵守資料保護規範，如：GDPR、PCI/DSS、HIPAA、GLBA、SB-1386 以及 US PII。

簡化管理、降低成本

- 藉由完全整合、集中管理的解決方案來提升掌握與監控。
- 採用單一代理程式來提供端點防護、裝置控管與資料外洩防護，降低資源需求與效能衝擊。

集中掌握與監控

- 與趨勢科技 Apex Central™ 整合來提供了一個方便的集中式防護管理主控台，將多套資料外洩防護解決方案的政策、事件與報表整合。

保護儲存中、使用中及移動中的資料

- 儲存中資料監控點：可辨識並處理 300 種以上的檔案類型，包括絕大部分的電子郵件與辦公室軟體、程式設計語言、圖片、工程檔案，以及壓縮、歸檔檔案。其發掘功能可掃瞄端點、檔案伺服器、郵件資料庫、Microsoft© SharePoint© Portal Server 資料庫、SaaS 應用程式以及雲端儲存來尋找法規要求的資料分散於何處。
- 移動中資料監控點：可讓您掌握及監控移動中的資料，包括：電子郵件、網頁郵件、即時通訊 (IM)、SaaS 應用程式，以及大多數的網路通訊協定，如：FTP、HTTP/HTTPS、SMTP。
- 使用中資料監控點：可讓您掌握及監控使用中的資料，包括：USB 連接埠、CD、DVD、COM 與 LPT 連接埠、可卸除式磁碟、紅外線與影像裝置、PCMCIA 以及數據機。此外還可監控複製/貼上及螢幕列印。

採用識別碼來提供精細的資料檢視

- 除了範本之外，Apex One™ DLP™ 還包含了真正國際化的識別碼詳細清單，可依據模式、公式、位置等等來識別資料。此外，也可從無到有建立自己的識別碼。

Apex One™ DLP™ 的優勢

防護點

- 立即保護您的資料。
- 立即部署資料外洩防護、立即掌握及監控您的資料。

降低資料外洩防護成本

- 相較於傳統的資料外洩防護，可節省部署與維護費用。

維護私密性

- 偵測、監控、預防資料外洩，不論裝置是否連上網路。
- 達成法規要求。
- 建置控管措施來保護、掌握及管制。

教育使用者

- 藉由通知來提醒員工注意一些危險的行為，或者在必要時強制實施使用者控管。

Endpoint Sensor

提供具備環境感應能力的端點調查及回應 (EDR)，詳細記錄系統層次活動並提供報表，以方便執行威脅分析，快速評估攻擊的性質和範圍。客製化的偵測能力、情報及監控讓您：

- 記錄詳細的系統層活動。
- 藉由豐富的搜尋條件，如：OpenIOC、Yara 及可疑物件在端點上執行多層次的搜尋。
- 偵測及分析進階威脅指標，如：無檔案式攻擊。
- 在資料外洩之前迅速因應。

Endpoint Encryption

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，而後兩者非常容易遺失或遭到竊取。趨勢科技 Endpoint Encryption 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、可卸除式媒體加密。

- 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、可卸除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。

趨勢科技 Apex Central

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，涵蓋多重環環相扣的趨勢科技防護層。此外，還可將掌握及監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，Apex Central™ 還可從趨勢科技 Smart Protection Network™ 取得可採取行動的威脅情報，藉由全球威脅情報從雲端提供即時防護，在威脅到達使用者之前預先加以攔截。

Security for Mac

- 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，包括一些針對 Mac 設計且快速散布的惡意程式。
- 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。

防護點

- 端點裝置
- 伺服器
- 內嵌式裝置和銷售櫃台系統 (POS)

威脅防護

- 漏洞攻擊。
- 惡意程式 (執行檔、DLL、裝置驅動程式、Windows® Store 應用程式等等)。
- 偵測、監控、預防資料外洩，不論裝置是否連上網路。
- 達成法規要求。
- 建置控管措施來保護、掌握及管制。

教育使用者

- 藉由通知來提醒員工注意一些危險的行為，或者在必要時強制實施使用者控管。

代理程式最低建議需求

代理程式作業系統：

- Windows 7 (6.1)
- Windows 8.1 (6.2/6.3)
- Windows 10 (10.0)
- Windows Server 2008 R2 (6.1)
- Windows Server 2012 (6.2)
- Windows Server 2012 R2 (6.3)
- Windows Server 2016 (10)
- Windows Server 2019
- macOS® High Sierra 10.13
- macOS Sierra 10.12
- OS X® El Capitan 10.11
- OS X Yosemite 10.10 或更新版本
- OS X Mavericks 10.9 或更新版本
- OS X Mountain Lion 10.8.3 或更新版本
- OS X Lion 10.7.5 或更新版本 (僅限 64 位元)

代理程式平台：

處理器：

- 300 MHz Intel® Pentium® 或同等級處理器 (Windows 7、8.1、10)；Intel® Core™ 處理器 (Mac)
- 最低 1.0 GHz (建議 2.0 GHz) Intel Pentium 或同等級處理器 (Windows Embedded POSReady7)
- 最低 1.4 GHz (建議 2.0 GHz) Intel Pentium 或同等級處理器 (Windows 2008 R2、Windows 2016、Windows 2019)

記憶體：

- 最低 512 MB (建議 2.0 GB)，至少保留 100 MB 給 Apex One™ 專用 (Windows 2008 R2、2012)
- 最低 1.0 GB (建議 2.0 GB)，至少保留 100 MB 給 Apex One™ 專用 (Windows 7 (x86)、8.1 (x86)、Windows Embedded POSReady 7、10 (x64))
- 最低 2.0 GB (建議 4.0 GB)，至少保留 100 MB 給 Apex One™ 專用 (Windows 7 (x64)、8.1 (x64)、10 (x64))
- Mac 上至少保留 512 MB 給 Apex One™

硬碟空間：

- Windows 至少 800 MB (建議 1GB)；Mac 至少 300 MB

如需更詳細的系統需求請至：docs.trendmicro.com

TREND MICRO™

Securing Your Connected World