AhnLab XTD

深入掌握 OT 資產與網路威脅

AhnLab XTD 提供 OT 網路的全面可視性，並即時偵測惡意流量與異常行為。

產品概述

AhnLab XTD 是專為 OT 環境打造的網路可視性與威脅偵測解決方案，可全面掌握 OT 網路狀況，並即時偵測惡意流量與異常行為。
透過系統化的可視性與威脅監控，XTD 能以最小化效能影響為前提，提供全面的網路監控能力。搭載深度封包檢測（DPI）技術，AhnLab XTD 可分析各種 OT 通訊協定與系統行為，協助管理員準確識別資產，並偵測 OT 資產設定或指令的異常變更。

可視性

資產可視性與通訊協定分析（DPI）
網路區段與拓撲分析

偵測

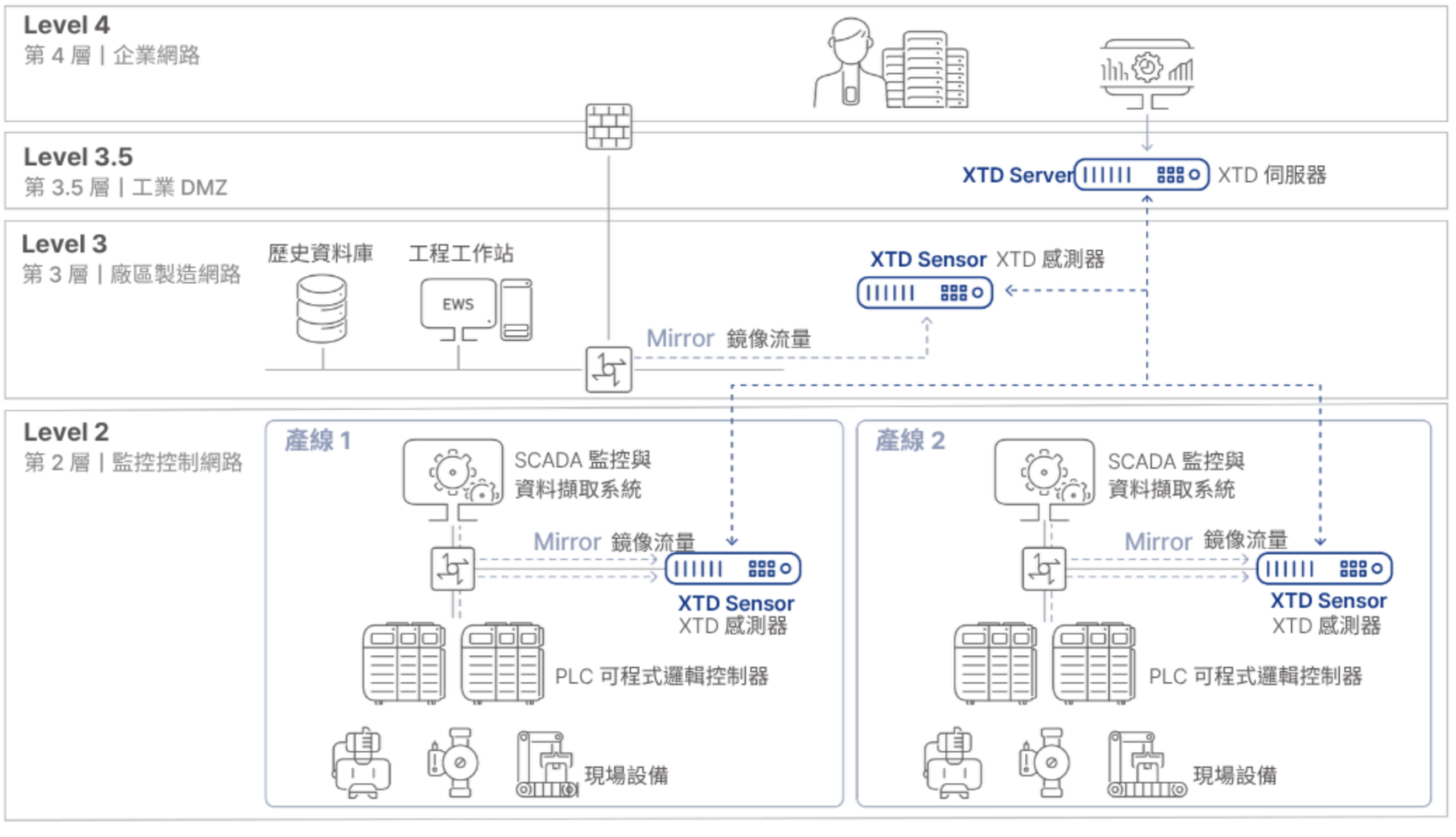
網路威脅偵測（惡意程式等）
異常協定與控制邏輯偵測

可用性

提供 Mirror（鏡像）模式
以維持系統可用性，無需變更網路設定

系統架構

AhnLab XTD 由中央伺服器與感測器（Sensor）組成，可部署於不同網路層級。XTD Sensor 部署於各 OT 網路中，負責分析鏡像流量（Mirror Traffic），並將分析結果轉送至中央伺服器；中央伺服器則處理所接收的資料，以識別網路威脅並套用適當的安全政策。
此外，AhnLab XTD 也提供全合一（All-in-One）伺服器配置，適用於規模較小的環境。



核心功能

可視性

即時掌握端點資產與端到端資產可視性，是保護實體系統（CPS）、OT 與 IT 網路，以及其網路資產的重要關鍵。AhnLab XTD 能分析 ARP、DHCP、IP 掃描及分析封包，全面掌握 OT 資產的可視性。

相較於競爭產品，AhnLab XTD 提供更深入且直覺的資產資訊，包括流量、網路連線與通訊協定分析（IT、OT、IoT），進一步提升可視性。

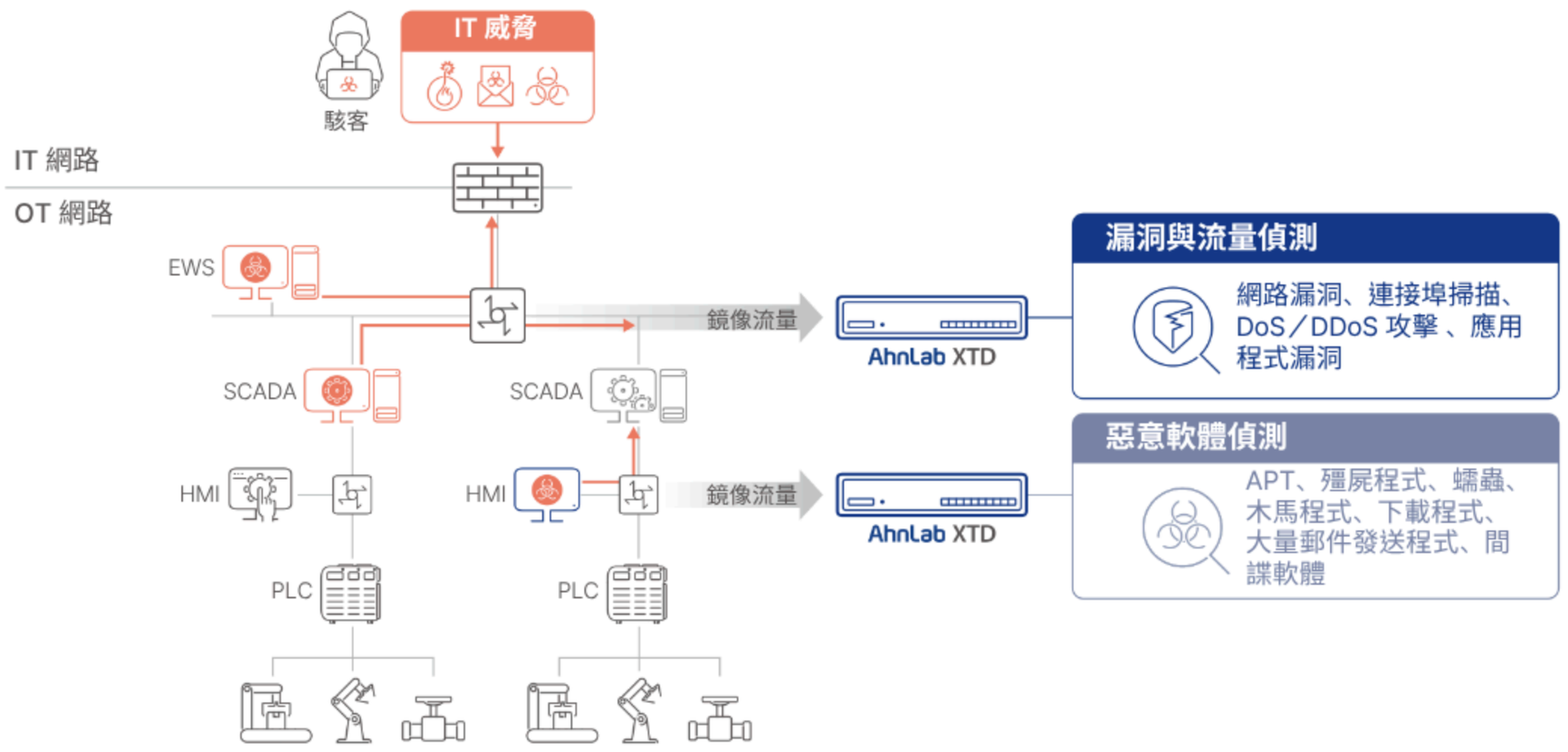
解決方案採用兩種操作模式（學習模式與運作模式），有效管理資產並偵測異常。在學習模式下，AhnLab XTD 會根據識別及登錄的資產，建立正常的資產行為基準。經過一定期間的資料學習後，可切換至運作模式，以加速資產識別與異常偵測。

威脅偵測

OT 網路通常採用高度隔離的方式部署，因此相較於其他網路環境，更容易受到網路威脅的影響。AhnLab XTD 採用先進的異常偵測與未經授權系統監控技術，提供安全的威脅偵測與監控能力。

AhnLab XTD 能成功偵測各種透過網路流量在網路中擴散的多元網路威脅，精準辨識和分析與勒索軟體、漏洞利用、資產探索及阻斷服務（DoS）相關的惡意活動，並向管理員發送警示。

透過業界領先的防毒引擎，AhnLab XTD 亦能提供最新惡意軟體的即時偵測能力。



異常偵測：行為基準

AhnLab XTD 透過深度封包檢測（DPI）分析各種 OT 通訊協定，建立異常偵測的行為基準。

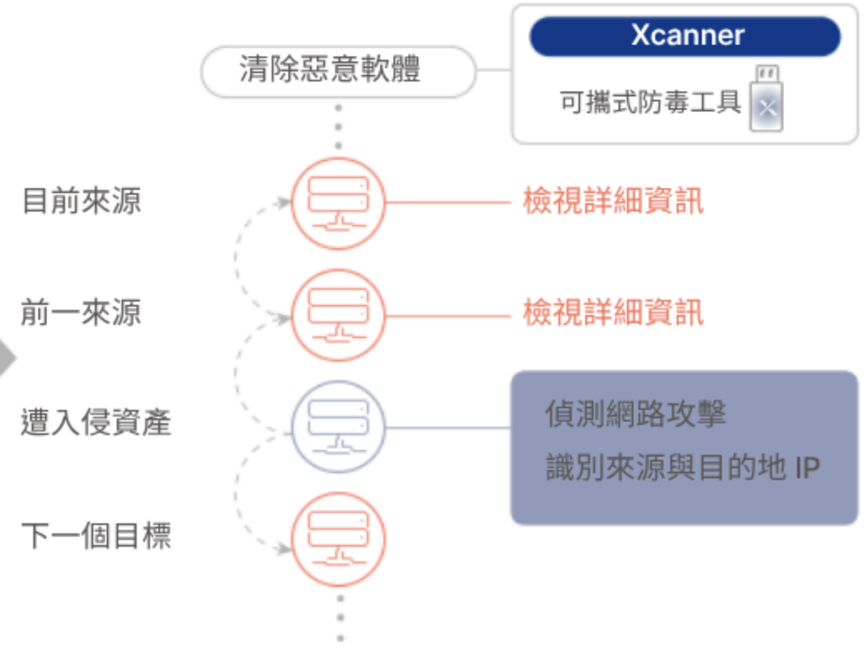
產品會針對管理員設定的製程數值進行統計學習，並據此建立正常的行為基準。當偵測到數值低於或超出基準範圍時，系統會將其判定為異常，並即時向管理員發送警示。

資安人員可即時掌握因系統故障或人為操作失誤所造成的異常，並迅速採取相應處置。

威脅追蹤

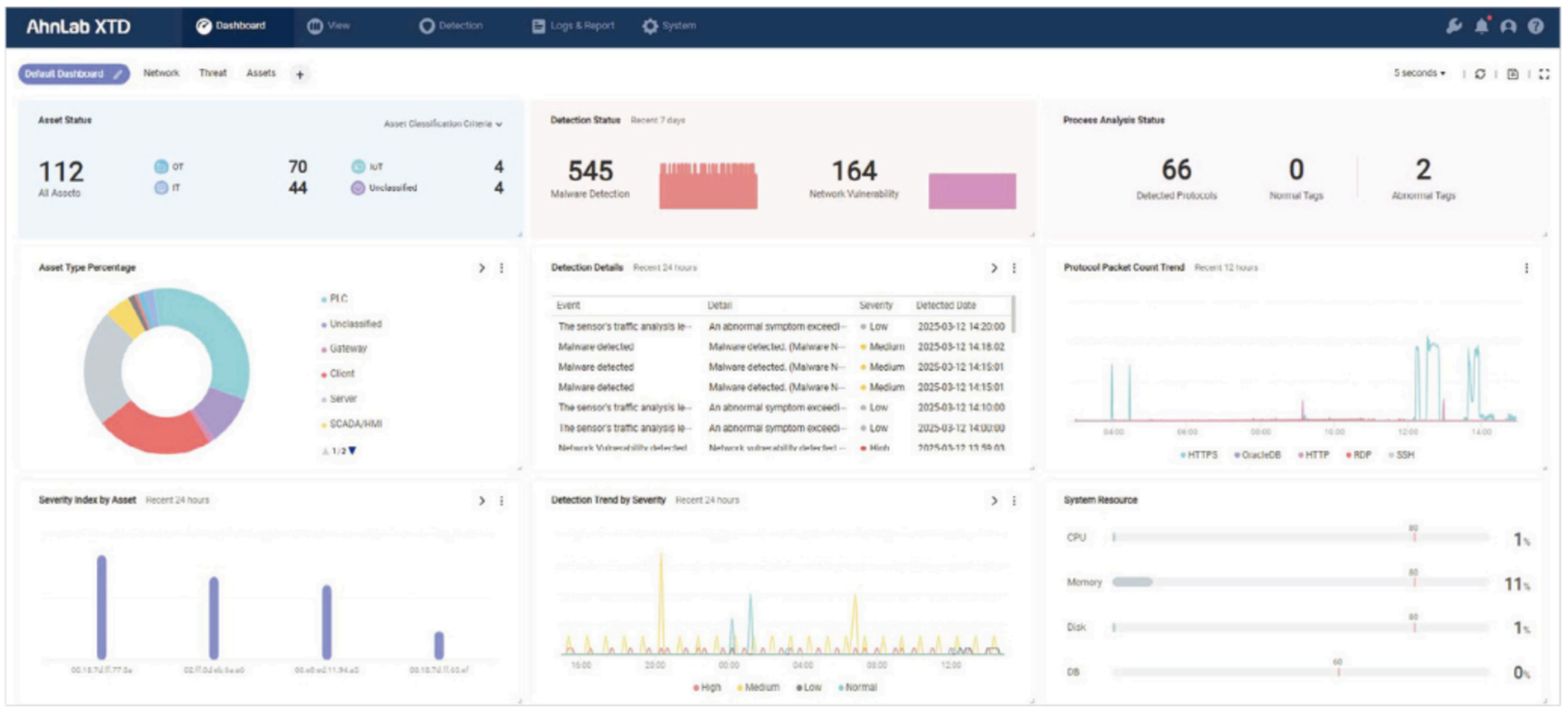
AhnLab XTD 可追蹤在 OT 網路中擴散的網路威脅來源，提升原本難以掌握之區域的可視性。
透過識別威脅先前的傳播路徑，使用者可以掌握網路威脅的移動軌跡，並採取主動防禦措施，避免下一個目標遭受入侵。
此外，管理員也可使用可攜式防毒工具 AhnLab Xcanner，掃描並清除受感染系統中的惡意軟體。

威脅追蹤示意圖



儀表板監控

AhnLab XTD 提供網頁式管理主控台及多項便利的管理功能，透過動態且直覺的儀表板，即時監控資產與網路威脅。
此外，管理員可依據實際需求，自訂儀表板的版面配置，透過獨立的面板（Panel）與小工具（Widget）建立及配置自訂儀表板，呈現所需的資訊。



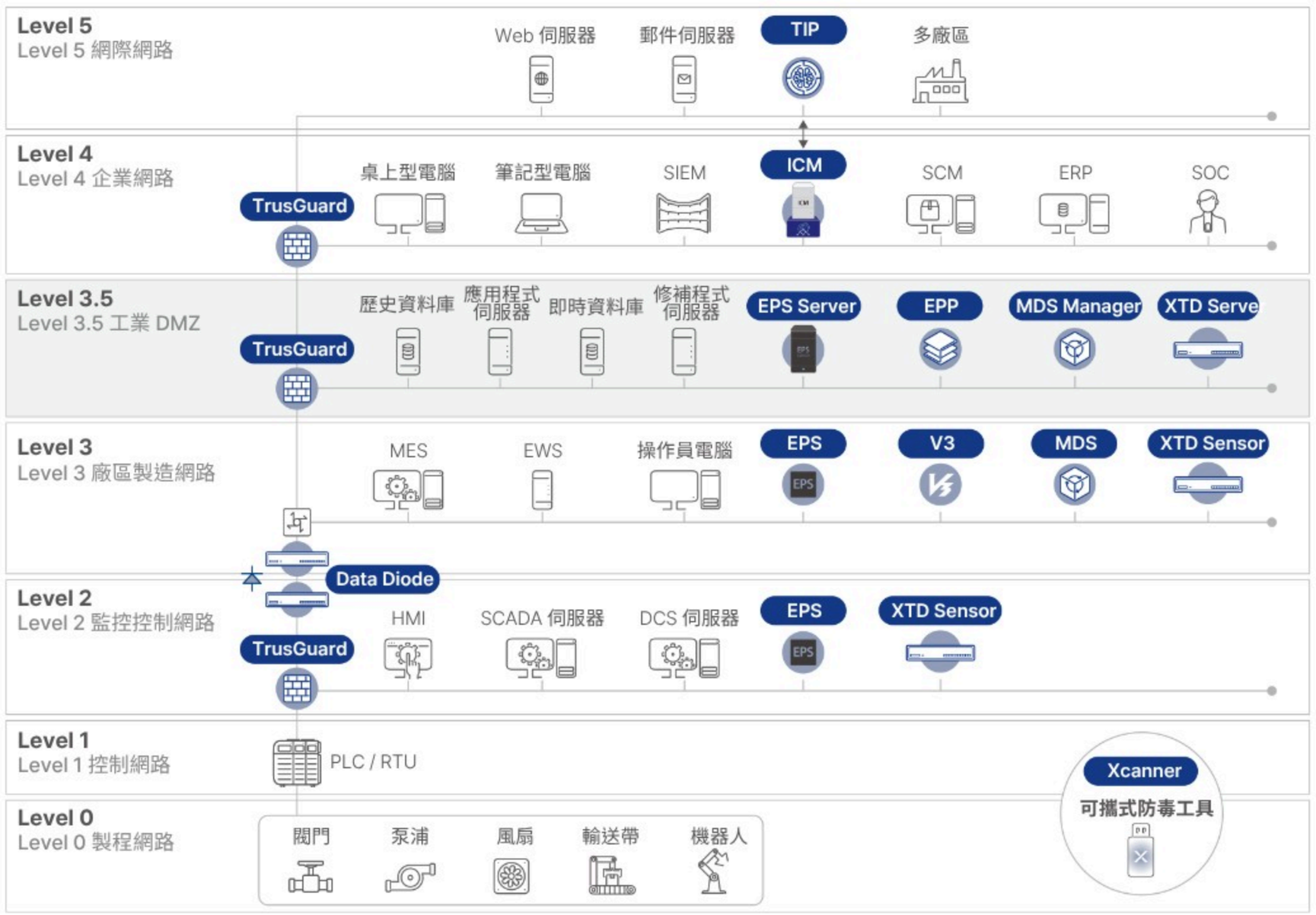
以平台為核心的 CPS 防護

AhnLab 長期提供 「AhnLab CPS PLUS」CPS 防護平台，針對 OT 端點、OT 網路，以及連接至 OT 環境的 IT 網域，提供系統化且完整的防護。

AhnLab CPS PLUS 結合 AhnLab 在威脅偵測與回應方面的專業技術，以及專為 OT 環境打造的安全技術，透過資產識別（可視性）、威脅偵測與威脅回應等能力，為客戶提供無縫且完整的 CPS 防護。

AhnLab CPS PLUS 所整合的各項安全模組，皆可透過中央管理解決方案 AhnLab ICM 進行集中管理與監控。

AhnLab CPS PLUS 提供業界最廣泛的 CPS 防護範圍，結合 AhnLab 卓越的資安技術，以及各安全模組之間順暢的整合能力，為客戶帶來更完整、更一致的 CPS 防護體驗。



端點－網路整合

AhnLab XTD 提供獨特的端點與網路安全整合能力，讓客戶能輕鬆享有其他產品難以提供的整合式安全防護體驗。這項強大的整合能力，來自 AhnLab XTD 與 AhnLab EPS OT 端點防護解決方案之間的無縫整合。

AhnLab XTD 可結合 AhnLab EPS Agent 所識別的端點資產資訊，偵測並驗證網路資產的可視性。此外，當 AhnLab XTD 偵測到網路威脅時，可透過與 AhnLab EPS 的整合，針對可疑系統即時啟動惡意軟體掃描，並利用 AhnLab Xcanner 進行處置。

台灣總代理 湛揚科技 T-Tech
台北市中山區民權東路三段58號15樓
www.t-tech.com.tw/ support@t-tech.com.tw