如何部署 OT 零信任防禦 確保高韌性廠務系統

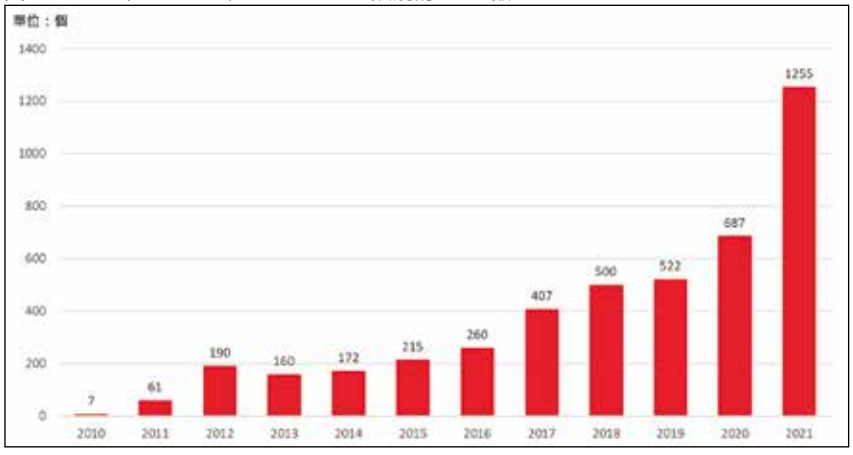
■文：TXOne Network Technical Marketing Team

駭客針對 OT/ICS 展開獵捕

工廠營運技術 (OT; Operational Technology)/ 工業控制系統 (ICS; Industrial Control System) 的數位安全在近年來遭受嚴峻的挑戰。據美國官方資料統計，自 2010 年至 2021 年 ICS-CERT 通報數量逐年增加，已累計通報達 4436 個漏洞，而且 2021 年漏洞通報數量創下歷年最高漲幅，突顯出駭客在 ICS 環境中能夠使用的潛藏武器庫日漸龐大 [1]。另一項調查顯示 [2]，從 2020 年 1 月到 10 月，勒索軟體攻擊案件中有 57% 發生在製造業或醫療保健業，且網路上大約每 14 秒就會發生一次勒索軟體攻擊。新型態的勒索軟體攻擊在台灣著名案例之一發生於 2020 年 5 月，當時有兩間台灣的主要石油供應商遭駭客攻擊。入侵者取得各公司的 Active Directory 管理員權限後，藉此散播 ColdLock 勒索軟體，導致總部的所有員工無法存取公司的線上系統，且客戶必須用現金才能加油，直到系統恢復正常。

傳統上營運系統防禦最常見的是依賴“實體隔離”(Air-gapped)，因此許多廠務管理者通常會假設營運系統是安全的，甚至許多 OT 系統的原始設備供應商在產品開發過程中完全沒有考量資安即設計 (Security by Design)，造成許多潛在資安風險。從著名的 Stuxnet、LogicLocker，以及 PIPEDREAM 等惡意程式攻擊分析，在面臨複雜的進階持續性威脅 (APT) 攻擊時，基於實體隔離的安全假設可能導致防禦部署的誤判，事實上許多 OT 環境並未完全與網路隔離，仍有機會被遠端入侵，甚至使得 OT 設備變成內部其他系統的攻擊性武器。

圖 1：2010 年至 2021 年 ICS-CERT 已識別的 CVE 數量



1. **存取控制權限洩漏**：此種攻擊最常利用社交工程或內部人員疏失，導致駭客獲得網路存取權限，駭客將利用機會特權升級，並橫向移動而不被發現，直到駭客找到關鍵的 OT 控制系統。例如：DoppelPaymer 利用含有魚叉式網路釣魚連結的垃圾郵件來滲透鴻海墨西哥廠，或使用或偽裝成正常文件的附件檔案，誘騙不知情受害者執行惡意程式碼。此程式碼再下載其他功能更強的惡意程式 (如 Emotet) 到受害者的電腦 [3]。
2. **軟體漏洞利用**：此種攻擊最常利用「軟體漏洞」來破壞目標廠務系統、流程或操作。駭客可以透過 Shodan 等漏洞搜尋工具

找到有弱點的攻擊目標，常見的是利用 OT/ICS 通訊協定上固有缺陷，例如：缺乏身份驗證和加密，跳過驗證機制來獲取遠端存取功能，最後在目標電腦上安裝惡意程式以發起各種攻擊。例如：2021 年肆虐全球的 Log4j 重大漏洞中，Cadence 部分產品遭受影響，故在已無法完全隔離的網路環境下，企業軟體伺服器也開始需要做好適當的內網的零信任管理 [4]。

3. **軟體供應鏈攻擊**：當駭客滲透到設備供應商的網路，並在供應商的產品交付給客戶之前，使用惡意程式破壞感染設備，此類型攻擊的特點是駭客在軟體編譯之前就滲透到供應商的軟體開發過程中，供應商的產品成為帶有惡意程式的軟體，例如：國家資助的駭客組織修改了 SolarWinds 的 Orion 網路管理軟體程式，在自動軟體安全更新中植入惡意程式，影響全球 18,000 名客戶。
4. **硬體供應鏈攻擊**：此類型攻擊主要透過篡改硬體，或修改供應鏈韌體來破壞設備。通常硬體操作在設備和外部電腦之間會建立一個“後門”連接，攻擊者會破壞該連接，一旦“後門”滲透到硬體供應鏈，駭客將使用它來獲得進一步的存取權限，或竊取資料。例如：國家資助的駭客組織 APT28 又被稱為 Fancy Bear（俄羅斯駭客組織）在 2018 年使用 UEFI rootkit 攻擊 Windows PC [5]。

OT 零信任架構須優先克服工廠環境挑戰

由於高度智慧化的工廠必須建立營運韌性，所有設備應確保營運生產不中斷。然而，傳統的 IT 資安方案並非專為 OT 環境所設計，它們並不能滿足工廠營運的環境需求，以下為常見的 OT 環境挑戰：

1. **老舊作業系統**：通常端點是 OT 安全中最薄弱的環節，因為 OT 設備的生命週期通常在 20 年以上，長期下來一座晶圓廠中可能存在 20 多個版本的作業系統，且每年都會有 1 至 2 個作業系統面臨停產問題。這些老舊作業系統的漏洞無法修補，容易成為 OT 資安的破口，例如：每個 Windows XP 或 Windows 7 系統都是易受攻擊的目標。
2. 安全更新困難：對於工廠的管理者而言，部署安全更新軟體可能是一項艱鉅的任務，因為要在 OT 環境中修補任何資產必須考量軟體相依性，以及相容性問題（修補後的資產是否與網路和其他資產相容），安排維護時程（何時進行此更新才不會影響生產），以確保生產流程的高可用性。
3. **複雜的 OT 通訊協定**：不同的產業在其工作場所會使用特殊 OT 網路架構與通訊協定，由於需求不同，它們可能有著很大的差異。此外，許多工業控制通訊協定並未加密，使駭客更容易操控工廠營運、干擾生產。
4. **內部 / 供應鏈威脅**：Air-gapped 環境之中所攜帶的行動設備，伴隨鬆懈的管理政策有機會讓惡意程式破壞 OT 環境或竊取敏感資料。例如：用於傳輸資料的 USB 隨身碟和用於維修的筆記型電腦，甚至任何一個供應商攜帶入廠的設備都可能成為惡意軟體傳播的完美載體。
5. **IT 資安方案不適用於 OT 環境**：在半導體設備產業中，端點會受特殊保固或法規的約束，而安裝額外的應用程式將會使保固無效或是違規。此外，製藥產業擁有許多此類資產，由於設備本身系統設計限制，也無法安裝防毒軟體，需要特殊的解決方案才能維護和保障此類系統。

如何部署 OT 零信任資安防護架構

承上所述，廠務管理者需要採用不同的方法，並遵循 OT 零信任原則：永不信任，始終驗證。採用 OT 零信任架構促使網路防禦永遠不會預設可信度，而且會不斷在網路上進行信任評估，並透過自動化方法實現 OT 零信任，橫跨應用程式、設備控制和網路，以確保生產力為最高優先順位。建議廠務管理者可運用資產生命週期方法來部署、實踐 OT 零信任資安架構，其中資產生命週期的四個關鍵階段，包含設備入廠、配置、生產和維護：

1. 入廠階段：

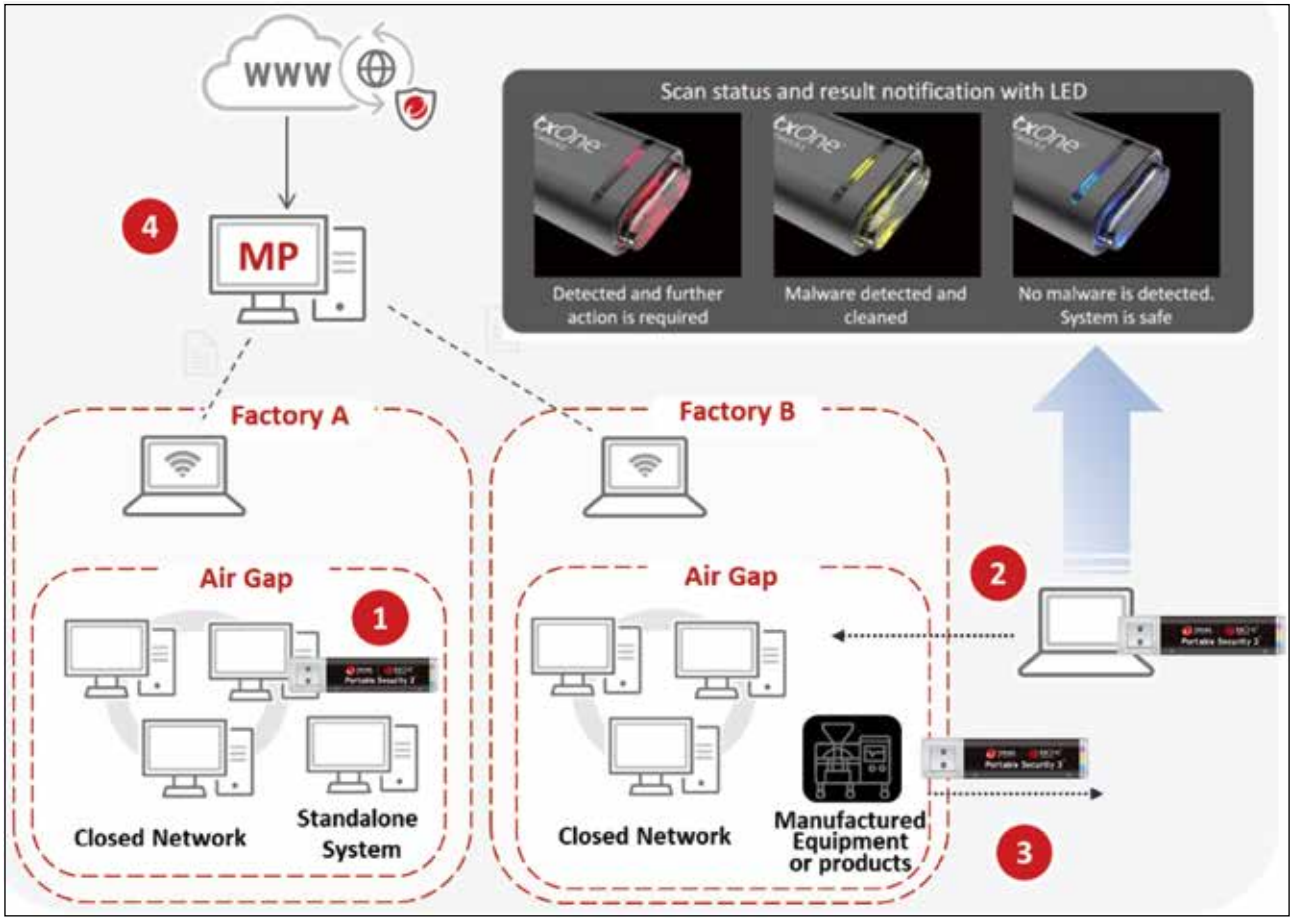
將資產運送到您的工廠設施

圖 2：借助資產生命週期框架部署 OT 零信任防禦

之前，供應商應掃描每項資產並建立 OT/ICS 健康記錄，以證明該設備不含惡意軟體。相當於國際航班出入境檢查方式，欲通過每個國家的海關時，任一側都必須在交易中為自己獨立確認設備的安全性。當每件設備到達工廠設施時，必須將其視為「有敵意」的設備，直到對其進行威脅掃描，並記錄任何潛在的可利用漏洞，類似於國際航班進出境時海關查驗，以確保設備不包含惡意軟件或嚴重漏洞。

目前半導體產業的資安標準 E187 要求設備入廠需要提出「無惡意程式證明」，TXOne Networks 建議可採用可攜式掃毒工具檢測供應鏈設備，以及訪客帶入產線現場的所有設備。特別的是 Trend Micro Portable Security 3 Pro 無須在端點設備安裝代理程式，解決過去無法在機台設備上進行掃毒的問題，且避免違反保固規定。此外，Trend Micro Portable Security 3 Pro 亦能在無網路的 air-gapped 環境執行惡意程式掃描，有助於半導體工廠針對供應商設備、維修人員電腦，以及定期執行資安稽核來確保供應鏈安全，緩解供應鏈攻擊，確保設備的完整性，同時符合特定產業的資安法規，如：

圖 3：使用可攜式掃毒工具檢查出廠 / 入廠裝置以保護工作現場



半導體資安標準 SEMI E187。

2. 配置階段：

配置階段是強固資產以消除攻擊手段的過程，包含防堵資安漏洞與關閉非必要服務，例如：應用程式、使用者權限、使用帳戶、網路埠和其他不需要的系統功能。通過強固資產，技術人員可以最大程度地減少攻擊者存取執行關鍵任務電腦，並阻止惡意程式運行的機會。半導體製程中目前仍有許多機台系統需要顧及安全，且絕不能危及日常操作、減慢運算速度，或延遲工廠生產過程中的決策，這些機台本身無法安裝 IT 所使用的防毒軟體，半導體設備商透過採用專門為 OT 環境所設計的 StellarProtect 工業級下世代防毒軟體，該功能運用 ICS 應用程式和憑證的資料庫進行過濾，該資料庫可驗證受信任的程式，消除不必要的資源消耗，以降低設備的營運負擔。在各種情境下它都保持有效、精準，而且對端點效能影響極小。StellarProtect 上的 ICS 應用程式保護功能則可確保 ICS 的完整性，以保護 ICS 免受針對性攻擊。為了防止無惡意軟體攻擊，StellarProtect 具有營運行為異常偵測能力，透過學習和授權操作的行為，並在最小權限控制下監控易受攻擊的正當流程。此外，StellarProtect 還可以透過 USB 裝置控管來防止內部威脅和內部惡意活動。然而，隨著時間的推移下現代資產將逐漸老化。針對老舊系統，StellarProtect 搭載獨特的信任列表和鎖定技術，以確保營運安全，包括：營運鎖定、USB 設備鎖定、資料鎖定和組態設置鎖定，可以完全保護複雜的老舊端點。最後，StellarOne 單一管理平台在整個資產生命週期中實現流暢管理。

3. 生產階段：

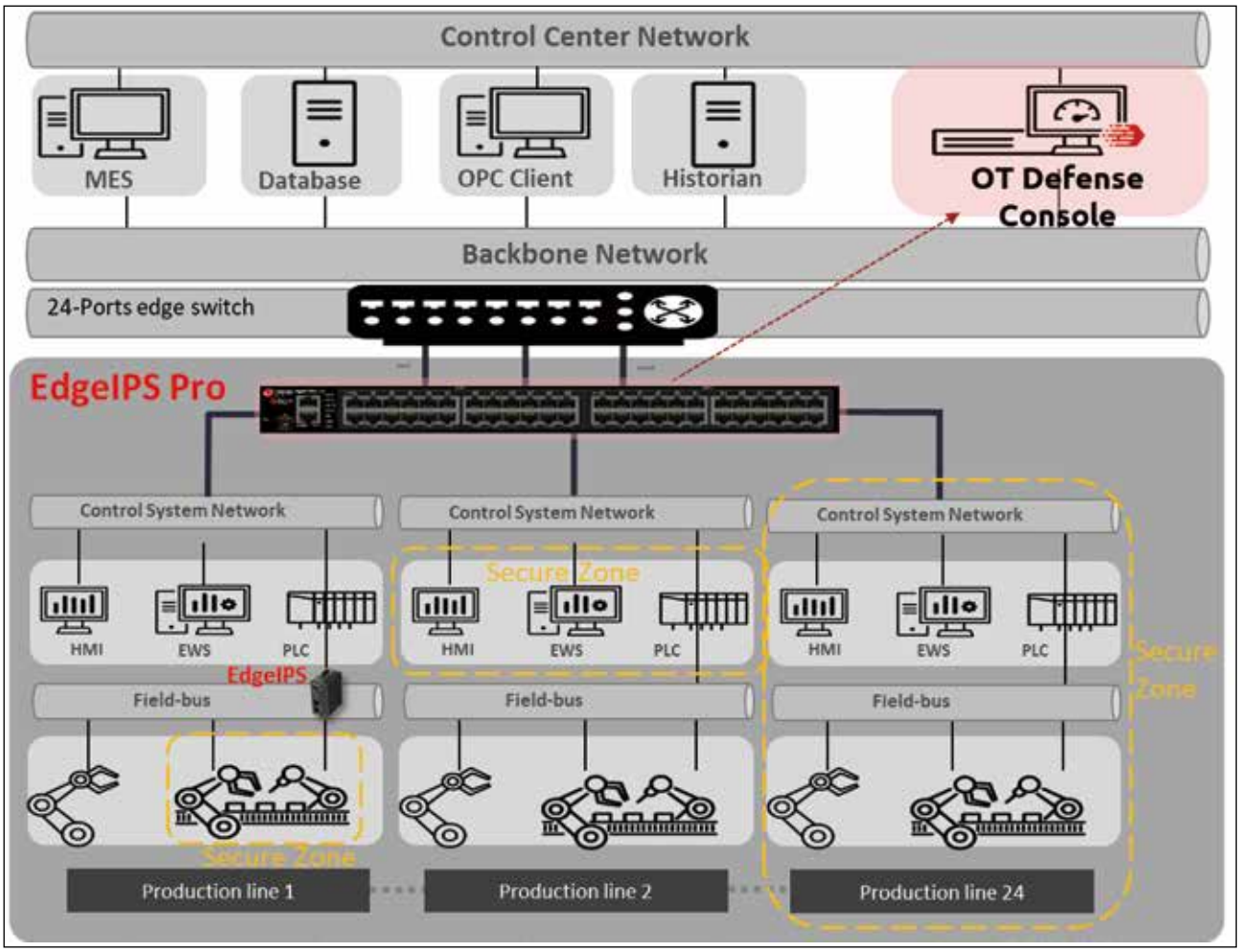
隨著資產進入生產階段，網路安全成為新變數。採用網段隔離技術成為部署 OT 零信任的關鍵。使用新一代 OT 入侵偵測系統或防火牆可以根據資產工作需要細分每個小區塊，然後將專屬的策略應用於每個小區塊，以照顧其中資產的特殊需求。工廠的管理者必須準備好抵禦駭客渴望利用網路散播的各種威脅，而分段利用改進的網路存取控制，以及更好的分析使防禦成為可能。在半導體工廠中透過部署專為 OT 網路零信任所設計的 EdgeIPS Pro 或 EdgeFire，可以協助工廠建立網段隔離、優化的網路存取控制和更好的入侵檢測分析，以便防止受損的 OT 設備演變成大規模災難，並使駭客在 OT 網路中收集資訊，或移動變得更加困難：

(1) 網路隔離技術：內部分段隔離 (Internal Segmentation) 和細部分段隔離 (Micro-Segmentation)。內部分段隔離適用於大規模範圍或區域，會根據可用的技術、頻寬和使用中的通訊協議來定義這個範圍。同樣地，細部分段隔離允許使用者將要保護的範圍或區域縮小到更小規模。透過 EdgeIPS Pro 或 EdgeFire 不需要更動現有網路架構，也不干擾現有網路配置，即可理解正常的操作流量。即使外圍網路控制鬆散 (如：允許從 Internet 存取 OT/ICS 設備)，EdgeIPS Pro 或 EdgeFire 也會阻止來自 Internet 的異常連接，並禁止受感染的 OT/ICS 設備進行橫向或縱向傳播感染其他 OT/ICS 設備。

(2) 虛擬補丁技術：透過主機式入侵預防系統 (Host-based IPS) 或網路 IPS 來建置。此類設備具有特別設計的規章，專門用於抵禦利用已知漏洞的攻擊，無需強制端點進行系統更新，意即不須重新啓動系統，亦不須讓產線停機。

圖 4：工業級下世代防毒解決方案確保 OT/ICS 完整性

圖 5：OT 原生 IPS 和防火牆實現高效率內部威脅偵測



(3) 網路信任清單：EdgeIPS Pro 或 EdgeFire 支援多種工業控制網路通訊協定與 L2-L7 網路流量的深度分析（如：MODBUS、Ethernet/IP、SECS/GEM、Siemens S7COMM 等），更提供通訊協定指令編輯與端點連接允許列表的操作建立出規則白名單。

4. 維護階段：

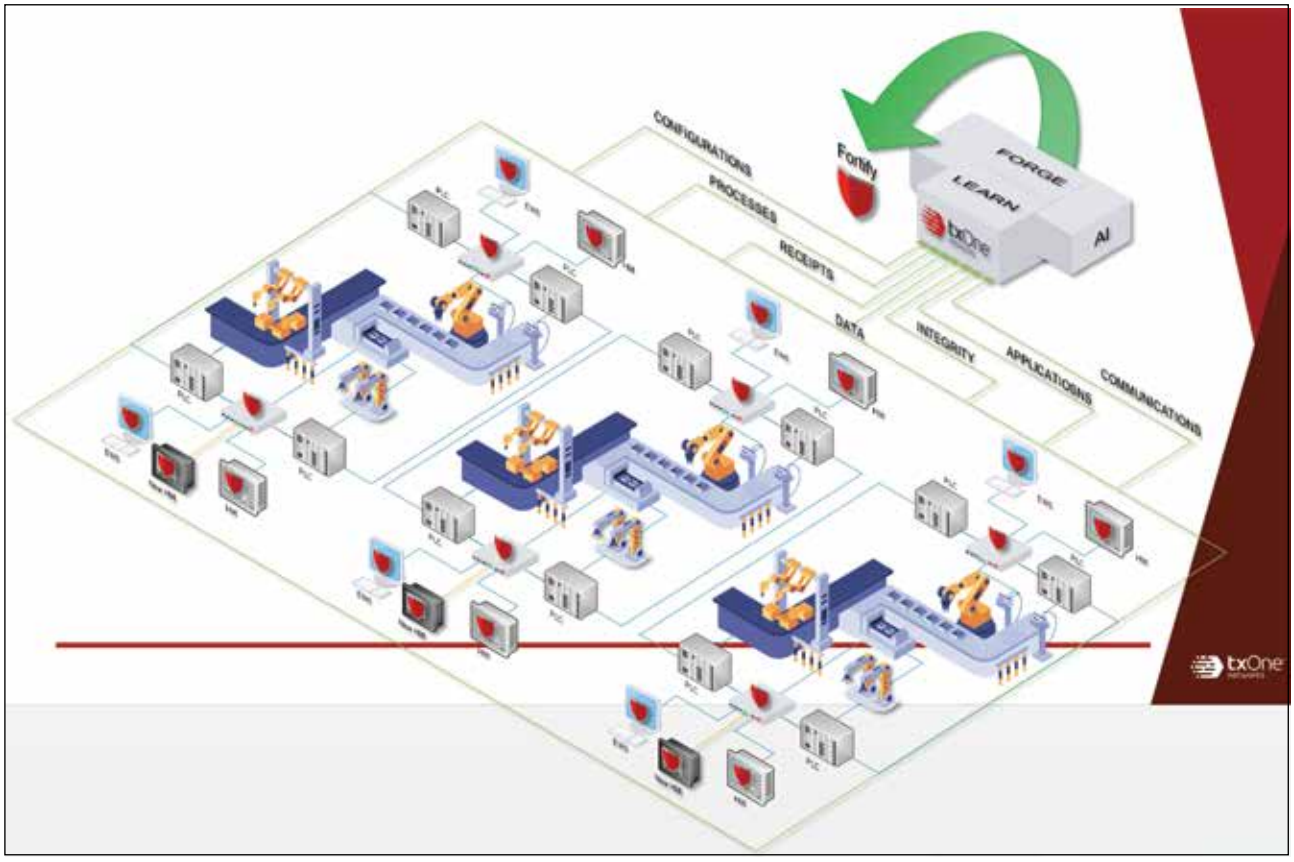
維護不僅意味著維修，還包括所有資產的態勢感知、軟體組態更改、系統升級和安全更新。透過持續性監測例行排程，結合 TXOne 的 AI 就會學習每項資產的複雜性，建立工廠單位所屬防護基準 (baseline) 來部署合宜的工廠防護方式，並確保工作場所流暢操作與營運持續性。TXOne Network 會將 OT/ICS 設備有關的資安日誌都集中到單個視窗中以供進行全面性態勢感知，或將資產配置資訊存檔提供給管理人員分析參考，其中包含：

(1) Management Program 則可收集的資產資訊，並透過集中管理程式以 CSV 格式作為資產清單發送到企業的 SIEM 或 Rsyslog 伺服器，以便於企業進行下一步的資產管理，例如：維護 OT 資產清單、識別惡意程式威脅，以及已知漏洞的資安風險。

(2) StellarOne 允許從單一管理平台進行管理，支援系統日誌轉發、入侵指標 (IoC) 蒐集與集中監控，讓資安營運中心更能掌握 OT 端點的資安狀況。

(3) OT Defense Console 透過儀表板來為工廠提供完整的 ICS 網路活動摘要，讓管理者得以檢視 OT 環境內安裝的所有 ICS 資產設備，以及它們的連線方式，並整理成告警、資產設備

圖 6：OT 零信任資安管理控制平台介面



與案件活動等不同摘要，讓管理者可直接監控資安狀態。此外，管理者亦可經由 ODC 從遠端執行所有節點的維護工作，例如：派送威脅特徵碼給 Edge 系列節點，或者編輯 OT 通訊協定信任清單，讓關鍵的生產設備彼此溝通互動。

從頭開始打造高韌性網路和端點

基於 IT 資安部署是不夠的，廠務管理者必須實施兼顧 IT 與 OT 的資安，解決 OT/ICS 工作場所獨特痛點才能夠確保建立營運韌性。TXOne Networks 建議透過資產生命週期的網路防禦觀點，協助廠務管理者滿足 OT/ICS 工作場所多樣多變且獨特的防禦需求，進一步部署更自動化、更全面的 OT 零信任資安解決方案，以便於建立供應鏈安全、現代與老舊的端點保護，以及複雜多變的網路防禦，確保廠務管理者簡化資安合規性、打造高韌性網路和端點，同時最小化對機台營運的影響。

參考資料：

[1] C. Max Farrell, Canaan Kao, Mars Cheng, Steven Hsu, YenTing Lee" TXOne Networks 2021 Cybersecurity Report", TXOne Networks, February 01, 2022

[2] Jacquelyn Bulao, "How Many Cyber Attacks Happen Per Day in 2020," techjury, July 28, 2020.

[3] Trend Micro," 剖析 FBI 向企業發出警告的 DoppelPaymer 勒索病毒" , Trend Micro, January 21, 2021.

[4] Cadence Security Advisory, "Log4j Vulnerability Security Advisory", Cadence, Accessed May 30, 2022

[5] NJCCIC Alert, "APT28: First Group to Embed Rootkit in UEFI", NJCCIC, October 02, 2018 CTA