TXOne OT 工控資安產品組合 2026

Keep the Operation Running.

Operations-First OT Security.

Discover.
Assess.
Protect.

txOne networks

與營運完美貼合的工控資安

TXOne Networks 是以營運為優先 (Operations-first) 的 OT 資安合作夥伴。我們打造以預防為核心、專為工業環境設計的資安防護，現已部署於超過 3,600 個營運場域並達成 100% 的營運持續性 (TXOne Networks 內部資料，2026)。企業不應被迫在滿足資安要求與維持生產運作之間做出選擇，因為在現實情況中，勒索軟體約在四分鐘內即可發動攻擊，而從偵測到防護執行的協調時間在最佳情況下仍需35至45分鐘，營運單位無法承受這樣的落差。我們的任務是在不改變既有營運模式的前提下消除這個落差，讓營運團隊再也不需要在資安要求與生產持續性之間做出取捨。

營運優先核心理念

全方位 OT 資安防護

我們提供全面性的 OT 資安防護，以單一原廠全面負責網路、端點、檢測與協同管理等層面，避免在資安事件中出現責任歸屬不清的情況，同時消弭整合負擔，並在整個 OT 環境中實現單一廠商的可視性與協同預防機制。

老舊系統延壽管理

我們協助企業保護既有 OT 資產而非強制汰換，支援從 Windows 2000 到 Windows 11 並承諾至少支援至 2031 年，亦支援現代控制系統所使用的 Linux，使企業能避免每套關鍵系統二百萬至五百萬美元的更換成本，並依照自身規劃的步調來排程系統升級，而非在危機中被迫升級。

不中斷營運的 OT 資安

我們透過硬體失效反制措施來確保資安設備的妥善率，以確保持續運作。用戶無需對環境設定進行修改、不需安排停機時間，也無需重新設計基礎架構，使資安能符合實際營運需求，而非對其造成阻礙。

3,600+
部署

100%
營運持續性

180+
工業協定支援

以及
40,000+
應用程式辨識
（TXOne Networks 內部資料，2026）

探勘 (Discover)、評估 (Assess)、防護 (Protect) 是我們實現 OT 資安的核心方法論。

TXOne Complete：單一優質夥伴 | 四大方針 | 以運營為本

沒有任何單一資安控制能夠端到端覆蓋整個工業營運環境，TXOne Complete 透過四種相互協同的防護策略橫跨 OT 生命週期，分別涵蓋設備進場前的資安檢測、防衛每個端點的正常運作、保護所有網路流量，以及在各個象限之間進行資安協同管理。每一個方針既可獨立運作，同時也可以在整合後發揮更強大的防護效果。

四大方針

設備進場資安檢測

在任何設備或儲存媒體接觸生產系統之前進行資安檢測，整個過程不需對系統進行修改，亦不需安裝代理程式，並完全支援不連網環境，專為外來設備、可攜式媒體以及受監管環境中的資產導入流程所設計。

端點可視性與防護

提供對所有 OT 端點的全面可視性與防護能力，不論是最新的 Windows 11 工程工作站到最舊的 Windows 2000 人機介面系統等，皆可透過以預防為核心的架構，自動建立每台設備的行為基準，並結合應用程式鎖定機制與 OT 專屬行為分析能力，同時提昇可視性及防護力。

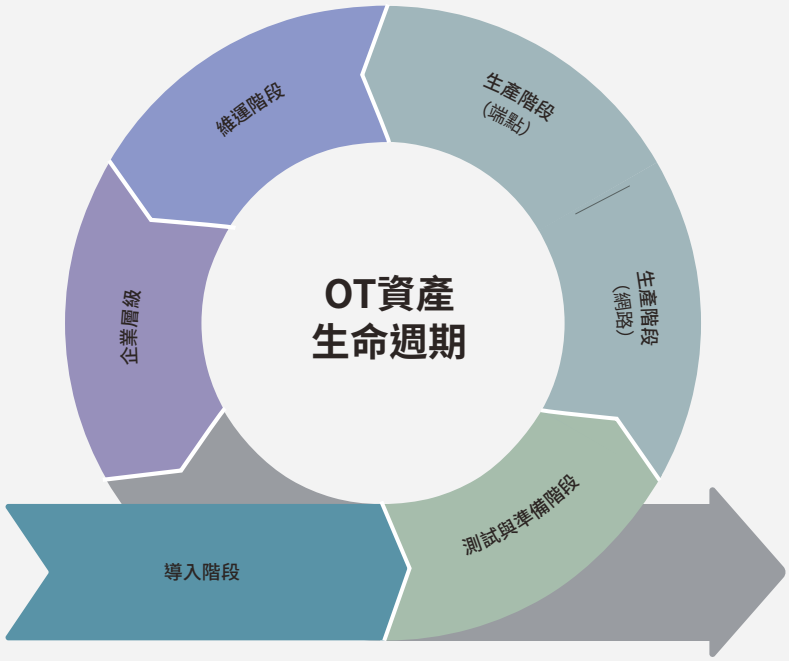
網路可視性與防護

在不需重新設計網路架構的情況下，實現對威脅的即時偵測與阻擋，透過極速的自動化防護能力以及硬體失效反制措施，確保營運不中斷，同時支援超過 180 種工業協定的深度封包檢測與指令層級控管，無縫保護所有設備，不論新舊，雨露均沾。

企業級資安協同管理

透過單一管理平台跨場域協調資安策略，提供整合式可視性、跨產品關聯分析以及以資產情境為基礎的風險優先排序，將資安發現轉化為營運單位可接受且可執行的修復計畫。

涵蓋完整OT資產生命週期



Lifecycle Phase	Operational Activity	How TXOne Helps
導入階段	在系統上線之前針對進場設備或是可攜式媒體進行資安檢測，確保所有進入環境的項目均符合資安要求。	Entry Point Validation
測試與準備階段	協助企業掌握現有資產狀態，並在進入正式生產前完成弱點評估與風險盤點。	Endpoint Visibility + Enterprise Orchestration
生產階段 (網路)	在網路層即時執行安全策略，阻擋未授權的指令與異常流量，確保生產環境穩定運作。	Network Visibility & Protection
生產階段 (端點)	保護作業系統並防止未授權程式執行，確保端點運作符合既定安全基準。	Endpoint Visibility & Protection
維運階段	在維護過程中保護受限的既有系統，同時對維修使用的儲存媒體進行安全掃描，避免風險導入。	Endpoint Visibility + Entry Point Validation
企業層級	透過跨場域事件關聯與策略協同，統一管理所有場域的資安狀態並強化整體防護能力。	Enterprise Security Orchestration

單一優質夥伴，四大協同防護策略，完整覆蓋 OT 資產生命週期的每一個階段。

設備進場資安檢測：
TXOne Element

在工業環境中，所有實體輸入如原料、工具、人員甚至包裝皆需經過驗證，而數位輸入同樣應遵循此原則。Element 能在不安裝代理程式、不修改目標系統且不需網路連線的情況下，驗證 USB 裝置、可攜式媒體以及外包商的其它設備，確保其在接觸生產系統前已通過安全檢查。

Element 產品組合

Portable Inspector（標準版與進階版）

Portable Inspector 為 USB 外型的可攜式掃描裝置，可隨時視需求進行媒體與資產檢測，具備多重惡意程式掃描與資產盤點功能，且不需在被掃描系統上安裝任何軟體。進階版額外提供 AES-256 硬體檔案加密，以滿足高規範環境中對於掃描流程可追溯性的需求。

Safe Port

Safe Port 為桌上型或壁掛式掃描站，適合在場域入口處進行進場設備及儲存媒體的資安檢測，其掃描速度可達每分鐘 7,200 個檔案。可戴手套操作的觸控螢幕與 LED 掃描結果指示設計，使無資安專業背景的操作人員亦能快速完成驗證流程。

ElementOne

ElementOne 提供集中式政策管理功能，可彙整掃描結果、生成合規報告、管理設備群組，並透過 REST API 與 SIEM 及 Sennin 整合，以提升企業整體可視性。

Element 核心價值

- 提供無需安裝代理程式的檢測能力，適用於無法接受軟體安裝的系統，包括已驗收過的既有設備與或是無網路的環境。
- 完全支援離線架構，可於遠端場域與隔離的生產區域中進行完整離線運作。
- 具備檔案鎖定功能，可直接在來源裝置上加密惡意檔案，防止其被意外再次導入系統。
- 透過LED指示的通過或失敗操作流程，使現場人員無需專業訓練即可完成所有入口驗證作業。
- 進階版本提供 AES-256 硬體加密，以滿足受監管環境對於防竄改稽核軌跡的需求。
- 可跨所有場域集中彙整掃描結果報告，涵蓋每所有設備以及每一次與外來設備的接觸。

每一個 USB 裝置、每一台外來設備，每一份可攜式儲存媒體，都必須在接觸您的系統之前完成資安驗證。

81.9%

的 USB 可疑活動來自檔案傳輸
(Nozomi Networks 2025 上半年 OT/IoT 資安報告)。

25%

的重大OT資安事件源自 USB 即插即用行為
(Honeywell 2025 資安威脅報告)。

1,826

種針對OT環境的獨特威脅類型在可攜式媒體上被偵測出來 (Honeywell 2025 資安威脅報告)。

端點可視性與防護：
TXOne Stellar

工業端點通常運行企業中最舊的作業系統，而傳統 IT 端點防護工具多假設具備雲端連線、現代作業系統以及 IT 專業人員管理，這些條件在 OT 環境中往往並不存在，Stellar 因此提供專為 OT 設計的端點資安解決方案，涵蓋從可視性建立到全面防護的整個成熟度歷程，並支援從 Windows 2000 到 Windows 11 以及 Linux 的完整環境。

Stellar 產品組合

Stellar Discover (new)

Stellar Discover 為僅提供偵測功能的端點感測器，其安裝時間約為一分鐘，不需驅動程式、不需核心存取且僅運行於使用者層，因此在架構上不會影響系統穩定性，並採固定價格授權模式支援無限數量部署，同時可與 IT 既有的 EPP 或 EDR 解決方案共存，提供裝置盤點、軟體盤點、弱點偵測、USB 活動監控、登入紀錄、網路流量記錄以及惡意程式活動回報等功能。

Stellar ICS Edition

Stellar ICS Edition 提供完整的防護能力，從最舊版本的 Windows Server 2025到最新的 Windows 11 全面無縫支援，同時支援 Linux 惡意程式掃描，功能涵蓋惡意程式防護、應用程式控制、USB 裝置控管、操作鎖定、CPSDR 行為異常偵測、自動建立設備基準、超過 40,000 種 OT 應用程式辨識、OT 應用程式與組態保護、網路存取控制以及無檔案攻擊防護。

Stellar Kiosk Edition

Stellar Kiosk Edition 為輕量版本，適用於資源受限或單一用途的端點設備，提供多引擎惡意程式掃描、USB 控制、操作鎖定與腳本攻擊防護。我們推薦在一般的情況下使用 Stellar ICS Edition， 若系統資源不足或是有其他的限制時，再退回 Kiosk 版本。

StellarOne

StellarOne 提供集中式政策管理、基準管理與合規報告功能，並支援從 Stellar Discover 升級至完整防護模式，且無需重新安裝或現場作業。

三大價值核心

營運導向設計

Stellar Discover 採使用者層運作且不存取核心，因此在架構上不會影響系統穩定性，而 Stellar Protect 則為每台設備建立行為基準，並阻擋所有偏離核准行為的活動，包括無檔案攻擊與利用系統內建工具的攻擊手法。

為 OT 環境而生

Stellar 支援免重開機部署與更新，具備極低的資源占用，並提供對營運安全的回應機制，同時涵蓋從 Windows 2000 到 Windows 11 的一致性防護，並承諾對舊版系統提供至少至 2031 年的支援。

資安防護不妥協

Stellar 採用多重防護架構，結合特徵碼、行為分析與啟發式偵測，並透過每台設備的行為基準與應用程式鎖定機制強化防護能力，同時支援不連網環境並已在超過 3,600 個場域中驗證其成效 (TXOne Networks 內部數據，2026)。

51%
的企業在過去 12 個月內曾發生舊版 Windows 資安事件。
(TXOne 2026 Legacy OT 資安報告)。

僅有 **39%**
為舊系統部署端點防護。

39%
企業表示 IT 端點工具會與 OT 營運產生衝突。

保護您現有的端點。延長其營運壽命。依照您的節奏來逐步更新系統。

網路可視性與防護：
TXOne Edge

勒索軟體約在四分鐘內即可完成攻擊，而從偵測到防護執行的協調時間在最佳情況下仍需三十五至四十五分鐘。僅具備偵測能力的平台雖能發現威脅，但仍需依賴其他機制進行阻擋，而當協調完成時，生產線往往已經中斷。Edge 從架構設計上直接消除這個落差，透過部署於網路流量路徑中，結合對超過 180 種工業協定的深度封包檢測，在極短時間內內完成威脅阻擋，並透過硬體旁路機制確保營運持續性。

Edge 產品組合

EdgeIPS

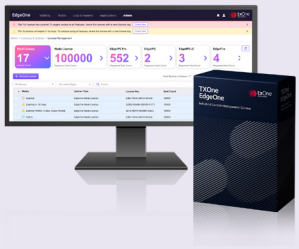
EdgeIPS 為串聯式 (Inline) 入侵防護設備系列，涵蓋多種機型，從用於單一資產保護的雙埠設備到用於核心網路的十六埠光纖設備皆包含在內，具備低於 500 微秒的延遲、硬體失效反制措施，並支援工業等級 -40°C 至 75°C 的運作環境與無風扇設計。

Sub-500
microsecond latency

EdgeFire

EdgeFire 為專為 OT 環境打造的次世代防火牆，適用於遠端場域，可於單一 DIN 軌設備中整合防火牆、IPS 以及點對點 VPN 功能，並支援超過 180 種工業協定的深度封包檢測與指令層級控管，具備 700,000 小時 MTBF 與工業級運作環境設計，特別適用於 IT 防火牆無法部署且偵測平台無法覆蓋的分散式場域。

180+
industrial protocols



EdgeOne

EdgeOne 為網路資安的集中管理與控制平台，每個控制台可管理最多 1,000 個節點，並透過 AI 驅動的自動規則學習，將原本需數月完成的策略設定縮短為數天，並支援 REST API、Syslog 與 CEF 輸出至 SIEM，並與 Sennin 整合以實現整體協同管理。

1,000
nodes per instance

Edge 核心能力

- 提供透明化的串聯式部署方式，不需配置 IP、不需重新設計網路架構，亦不會造成生產停機。
- 支援超過 180 種工業協定的深度封包檢測，並可於第二層與第三層執行指令層級過濾。
- 提供系統無關的虛擬補丁機制，可保護無法更新的設備，無論新舊。
- 具備多層次故障反制措施，在資安事件中確保最高營運持續性。
- 提供多種工業級設備型態，以滿足不同場域規模、預算與任務需求。
- 提供完整連線、資料流與協定指令層級的可視性。
- 支援資安節點的集中管理與策略協同部署。
- 透過 AI 驅動的流量分析，協助精簡 OT 團隊的資安設定工作。

以極速的即時防護可來有效彌補四分鐘攻擊落差。而多層次故障反制措施則確保在防護過程中維持生產不中斷。

企業級資安協同管理：
TXOne Sennin

每導入一套新的OT資安解決方案，往往就會增加一個新的管理平台、一套新的政策，以及對專業人力的新需求。Sennin 將 TXOne 全產品線的資安資訊整合至單一平台，透過集中式治理架構統一可視性並以營運情境優先排序弱點，使企業能在單一平台上掌握整體資安狀態、協調回應並驗證資安成效。

2026 年 4 月推出的 Sennin 3.0 版本透過兩大相互協同的運作模式來展現其核心價值，分別為針對已具備成熟資安計畫並持續擴展的企業所設計的「策略治理（Strategic Governance）」，以及針對正在建立或重整 OT 資安計畫的企業所提供的「探勘與評估（Discover & Assess）」。

用SenninOne達成策略性的資安治理

SenninOne 為針對已部署 TXOne 解決方案的企業所設計的資安調查與協同管理平台，能跨場域、跨產品與跨資安團隊進行集中管理，將隨企業成長而產生的管理複雜性轉化為營運優勢。

- **跨產品關聯分析。** SenninOne 支援 MITRE ATT&CK for ICS 對應，並可跨 Edge、Stellar 與 Element 進行事件關聯分析，使威脅調查能結合營運情境而非僅依賴單一警示，可同時支援小至 500 大至 100,000+ 的資產管理，並可與 Splunk、Microsoft Sentinel 與 QRadar 等 SIEM 雙向整合。
- **符合營運流程的核准機制。** 系統提供角色基礎存取控制與針對 IT 與 OT 的客製化建議，確保所有策略部署皆需經過營運單位核准，使 IT 與 OT 之間的協作流程具備結構化、可追蹤與可稽核的特性。
- **企業級資產安全態勢。** 提供跨所有場域與產品的資產覆蓋率、健康狀態、風險程度與生命週期概覽，使企業能隨時掌握單一且最新的整體資安狀態。

三大治理核心

資產安全態勢

提供所有端點、設備與入口的覆蓋率、健康狀態、風險與生命週期的整體視圖。

權重式弱點管理

透過 VSAR 機制依據營運情境而非僅依 CVSS 分數進行弱點優先排序，提升風險處理效率並確保方案可被營運單位接受。

情境導向 OT 資安

透過多來源資料整合、CPS 偵測與回應以及具行動性的洞察分析，將營運情境與資安控制回饋有效串聯。

67%
的企業在 IT 與 OT 可視性整合上面臨困難。

33%
的 OT 資安事件發生於 IT 與 OT 整合點。
（Omdia 與 TXOne 調查數據）

71%
的企業偏好採用單一廠商 OT 資安平台
（Omdia 與 TXOne 調查數據）

對於尚未建立 OT 資安計畫的企業，則可從 探勘 (Discover) 與 評估 (Assess) 階段開始導入。

Discover + Assess: TXOne SenninRecon

企業無法保護其無法掌握的資產，在建立資安防護之前，企業需要完整的資產盤點、可信的風險評估以及營運單位可接受的修復計畫，而這正是 Discover 與 Assess 階段的核心價值，SenninRecon 即為此階段的關鍵解決方案，並可與 SenninOne 及 Stellar Discover 搭配，在單一專案中將 OT 資安從概念轉化為具體可執行且可獲得預算支持的計畫。

SenninRecon：以 VSAR 為基礎的評估導入入口

自動化資產發現

透過被動式方式跨場域與網路區段進行資產盤點，不需安裝代理程式亦不需串聯部署，即可在不影響生產的情況下完成資產探勘。

VSAR 弱點評估

透過營運情境進行弱點評分，使風險排序更貼近實際營運影響，例如低風險系統上的高嚴重性漏洞可能優先度低於關鍵系統上的中等漏洞。

可執行修復計畫

提供具優先順序且可執行的修復建議，避免產出冗長且難以落實的弱點清單，使資安計畫更容易獲得預算支持。

Recon + Discover 整合

對於尚未建立資產盤點的企業而言，SenninRecon 通常會與 Stellar Discover 搭配，在 Discover 階段以整合專案的方式導入，透過 SenninRecon 所提供的網路層可視性與 Stellar Discover 所提供的端點層可視性相互結合，形成市場上唯一可實現端到端 OT 資安態勢盤點的流程，且在整個過程中無需現場進駐、無需修改系統，也不會對生產造成任何中斷。

- SenninRecon 可呈現網路層級的資產資訊、流量行為模式以及可從網路觀測到的弱點風險。
- Stellar Discover 提供端點層級的軟體資產盤點、各端點弱點狀況、USB 活動以及主動惡意程式回報。
- SenninOne 負責整合上述兩個層面的資料來源，套用 VSAR 評分機制並產出具優先順序的修復計畫。

一次專案導入即可獲得完整可視性，並為下一階段資安投資提供具體且可量化的依據。

為何評估至關重要

47%
有 47% 的企業指出其在 OT 技能與資源方面存在明顯缺口。
(PWC 2025 全球數位信任洞察報告)。

10%
僅有 10% 的企業將 OT 資安列為前三大預算優先項目。
(PWC 2026 全球數位信任洞察報告)，而以證據為導向的評估之所以能有效解鎖預算，是因為它能將原本抽象的風險轉化為具體量化且具優先順序的發現。

29%
僅有 29% 的關鍵基礎設施組織具備集中式資產管理能力。
(Bridewell 2026 CNI 資安報告)。

TXOne SenninRecon

維持營運不中斷，從 SenninRecon 的被動式評估開始。該過程無需代理程式、無需網路變更且不會影響生產。您可以與我們安排一場 60 分鐘的價值驗證測試，亦可直接與您的 TXOne 團隊聯繫以展開進一步討論。