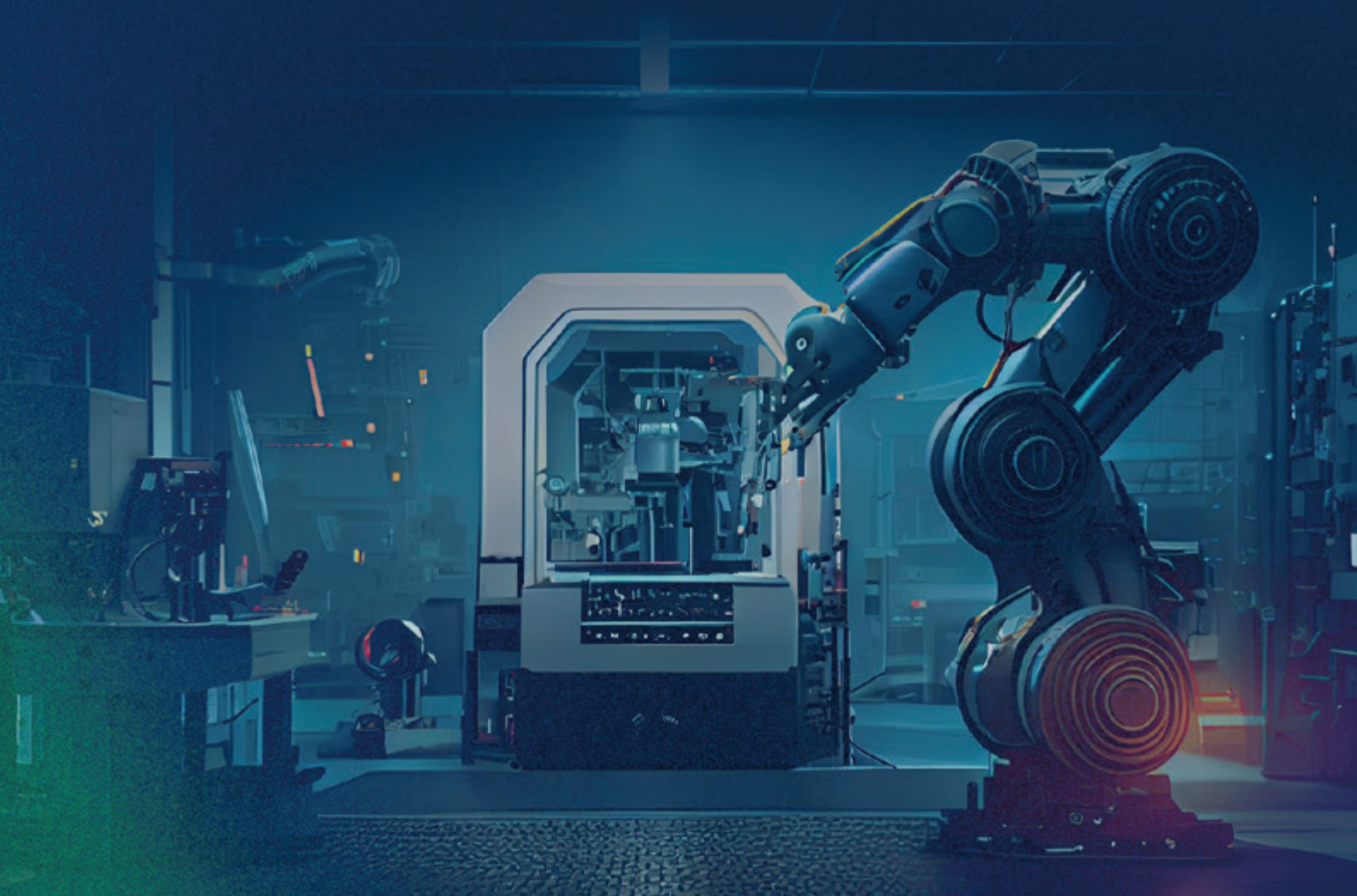
tenable

製造業工作場所的網路安全



目錄

在製造業中運用數位化

在製造業中運用數位化可追溯至早期的自動化，在這個時期，製造業者初次開始使用電腦系統來管理及控制生產程序。從這個時候開始，數位轉型便完全革新了製造業工作場所，不僅能提高效率和生產力，同時還改善了品質控管、降低成本並增加彈性與客製化能力。隨著工業 4.0[1] 降臨，企業變得更加靈活、互連性更高且更加以資料為導向，使企業能夠適應瞬息萬變的市場需求。

根據 Deloitte 顧問公司所發布的一份全球研究，製造業者在建置智慧型工廠數位化措施之後，觀察到在生產輸出方面增加了 10%、在產能利用率方面增加了 11%，且在人員生產力方面增加了 12%。此外，製造業者還能將創新開發時間降低達 30%[2]，藉此加速新產品上市。製造業者紛紛採用數位轉型，因此能夠在日益競爭且變化莫測的市場中透過自我定位來獲致成功。

然而，數位化的優勢往往需要付出代價。根據 Deloitte 的 2023 年製造業展望，網路攻擊將持續成為 2023 年的重大挑戰[3]。當製造業者採用越來越多網路連線技術，隨之而來的是新型且通常是前所未見的挑戰，使得生產力和安全性顯得岌岌可危。若對於您工作場所的操作技術 (OT) 生態體系以及支援您工作場所的 IT 系統沒有透徹的能見度和掌握度，以及正確的防護各就各位，您的挑戰就只會更加複雜並且破壞貴公司的製造業運作。

數位化所帶來的網路安全挑戰

先進的數位系統與互連網路的整合已使工廠轉型成複雜的虛實整合環境。儘管這場數位革新很有希望帶來巨大的利益，但也必須解決許多隨之而來的挑戰，才能確保製造業運作的安全性和穩定性。

這些挑戰包含：

攻擊破綻擴大：工廠數位化會使攻擊破綻擴大，讓網路罪犯更加有機可乘。在使用互連裝置、感應器和系統之際，有越來越多潛在的弱點可能會遭到刺探利用，進而增加網路攻擊的風險。

舊系統和虛實整合系統中的弱點：許多製造業的設施仍然仰賴舊系統和舊設備，而這些舊系統和舊設備往往缺乏新型的安全控制機制。將這些系統與新的數位技術整合可能會造成相容性的問題，並且曝露弱點而成為網路攻擊者的目標。許多 OT 系統都因修補程式所需的停機時間而無法定期更新。事實上，有 47% 的製造業網路入侵都歸咎於弱點遭到攻擊者刺探利用[4]。一旦您得知環境中的弱點之後，接下來的挑戰就是瞭解要優先修復的弱點。

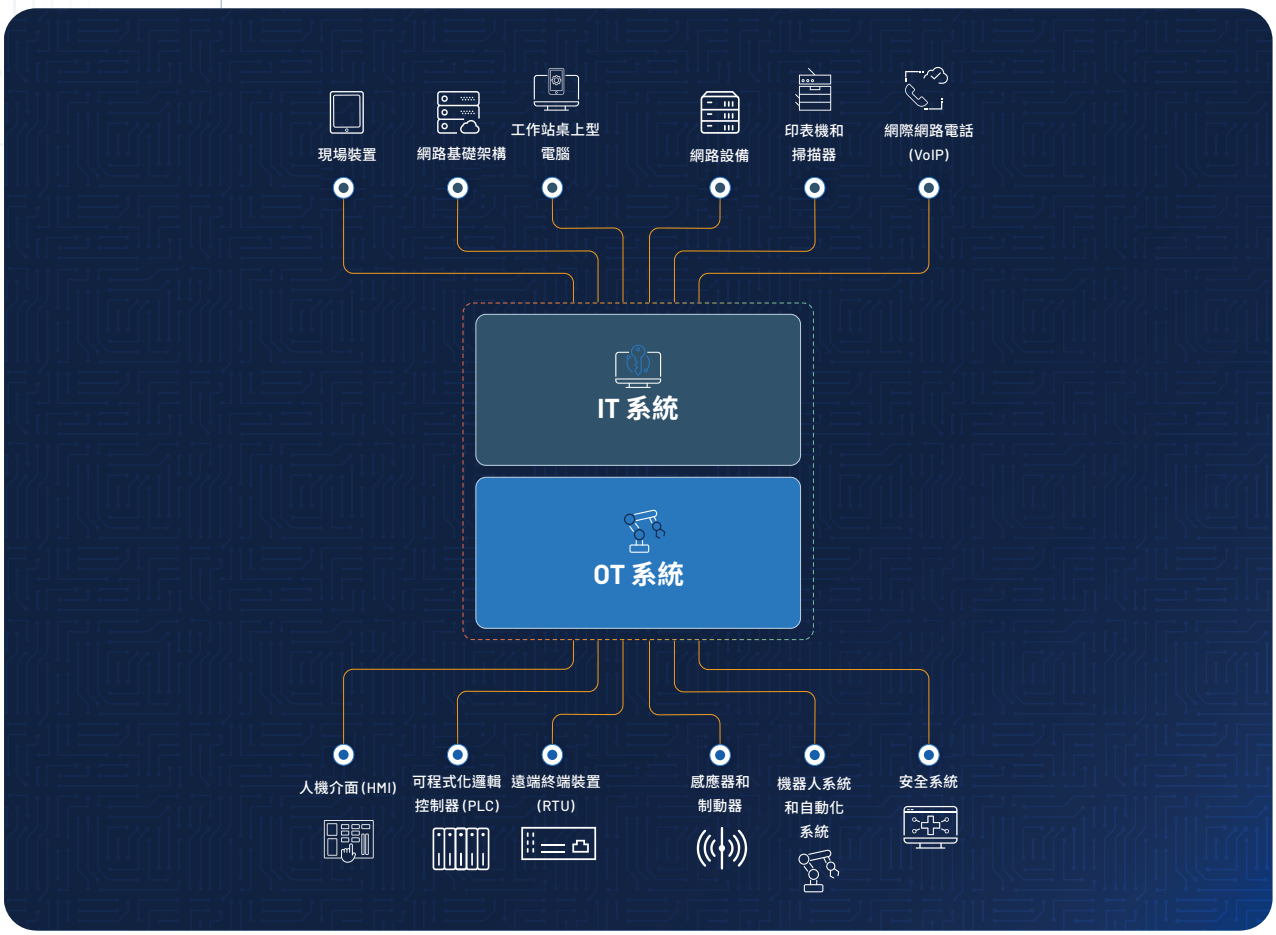
內部人員造成的威脅：數位轉型程序通常涉及工作團隊角色、技能要求和存取權限中的變更。惡意的內部人員或是不慎破壞安全措施的人員都可能會對製造業運作造成極大的風險，因而導致非計劃性停機。視企業的規模和特定產業而定，非計劃性停機每小時的生產力損失成本可能介於 90,000 至 640 萬美元之間。大部分的企業 (98%) 都宣稱，光是一小時的停機時間成本，就超過每小時 100,000 美元[5]。

日新月異的威脅態勢：製造業者在採用數位技術之際，儼然成為各種網路威脅的攻擊目標，這些網路威脅包括勒索軟體、網路釣魚攻擊、產業間諜活動和由民族國家支持的攻擊。

互連網路導致各種挑戰和風險，這類互連網路擴及工作場所，且對於尋找攻擊目標的威脅執行者而言代表著極高的價值。為保障生產線的完整性和功能性，務必要瞭解這些威脅的位置並建置強大的安全措施。

製造業環境中可能發生威脅之處

製造業環境通常包含複雜的 OT 與 IT 互連裝置生態體系；OT 負責自動化生產，而 IT 負責管理 OT 系統。IT 裝置可能佔了現代製造業環境的一半。請務必瞭解資產組成並採用解決方案廠商，能在您的 IT 和 OT 環境中為您提供完備的涵蓋範圍及安全。對 OT 系統的威脅可能包含未經授權的存取、竄改、惡意軟體、韌體或軟體中的弱點遭到刺探利用，以及社交工程攻擊。對 IT 系統的威脅可能包含惡意程式碼、竄改、韌體或軟體中的弱點遭到刺探利用、網路入侵、拒絕服務 (DoS) 攻擊以及惡意軟體。



以上清單未盡完整，僅為您提供參考架構，瞭解製造業環境中的攻擊破綻數量遠比預期更多。這涵蓋安全團隊必須盤點並且時刻掌握能見度的資產。威脅執行者會靜靜等待並伺機刺探利用 IT 和 OT 裝置上的弱點，做為中斷點及潛在的起點來穿越企業的公司網路，反之亦然。

保護工作場所 IT 和 OT 的需求

為降低您製造業運作中斷和入侵資料的風險，製造業者在其數位轉型計畫中，必須將網路安全視為當務之急。保護 OT 環境需要採取全方位的方法，這種方法牽涉到結合技術控制、原則及程序，來將網路攻擊得逞的風險降到最低。

製造業者應持續評估其安全態勢，並且在建置 OT 安全策略時，考量將下列項目納入基本功能：

資產庫：IT 和 OT 裝置的能見度（包含其型號、系列、類型、韌體版本、作業系統版本、硬體版本和序號）對於在製造業環境的攻擊破綻中，正確清查所有資產至關重要。

弱點管理：弱點管理對於在混合新型和舊型系統的製造業環境中維持主動且有效的網路安全方案而言至關重要。

威脅偵測：製造業環境中的入侵偵測功能對於及早發出威脅警告、探索內部人員造成的威脅以及偵測惡意軟體而言必不可少。額外補充：這項功能有助於減少非計劃性停機時間的可能性。

設定管理：威脅態勢不斷日新月異，監控裝置設定儼然成為不可或缺的功能。人為錯誤或可能的惡意活動都可能會造成非計劃性停機時間，因而對製造業生態體系的安全和生產力造成威脅。

製造業者首重營運持續不中斷和效率。生產過程中發生任何中斷都可能會帶來嚴重的財務後果。由於製造業環境中 OT 裝置在本質上皆屬敏感，因此傳統的網路安全工具可能會產生誤報問題或造成停機時間。因此，IT 型網路安全工具對生產過程可能會造侵入或中斷。要解決網路安全挑戰，就需要針對複雜的 OT 環境所明確設計的專用解決方案。

「在網路攻擊事件中，往往不僅要專注於**網路防禦**，還要專注於業務穩定性和持續不中斷。**日益增加監控措施**來盡快查看資訊科技和操作技術的異常行為，能夠避免災難性的傷害。」

資料來源：Deloitte，2023 年製造業展望，2022 年 8 月。

TENABLE OT SECURITY 對製造業者有何幫助

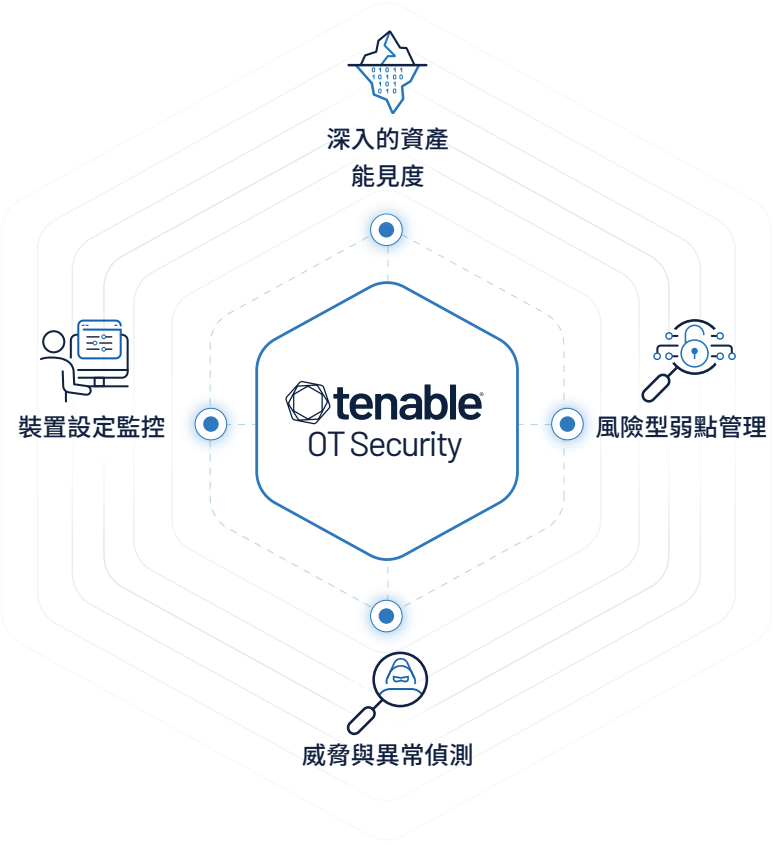
Tenable OT Security (前稱 Tenable.ot) 是市場首屈一指的網路安全解決方案，專為保護複雜的 OT 環境所設計，專注於保護掌控實體處理流程的網路。Tenable OT Security 特別針對解決 OT 系統的獨特需求和挑戰所設計，讓製造業者能夠即時偵測威脅，並回應網路安全資安事端。

內含的特點和功能包括：

深入的資產能見度

Tenable OT Security 在環境中提供專業化 OT 和傳統 IT 裝置的能見度，可查看集中化的製造業攻擊破綻檢視畫面。同時看見兩個網域使企業能夠全方位地監控、管理並保護其整個基礎架構。此外，還能讓企業找出所有進入點以及可能有弱點的連結，網路攻擊者可能會利用這些進入點和連結來嘗試取得未經授權的存取或刺探利用弱點。

Tenable OT Security 會使用混合資產搜尋方法，進行被動監控來搜尋透過網路進行通訊的裝置，並在進行分類後，利用 Nessus (Tenable 的旗艦弱點掃描器) 來掃描 IT 資產，同時使用其原生通訊協定安全地查詢 OT 資產。Tenable OT Security 可對應所有連線裝置、系統和網路元件，追蹤韌體和作業系統版本、內部設定，執行軟體和使用者資料，以及 IT 和 OT 設備的序號和底層設定。



風險型弱點管理

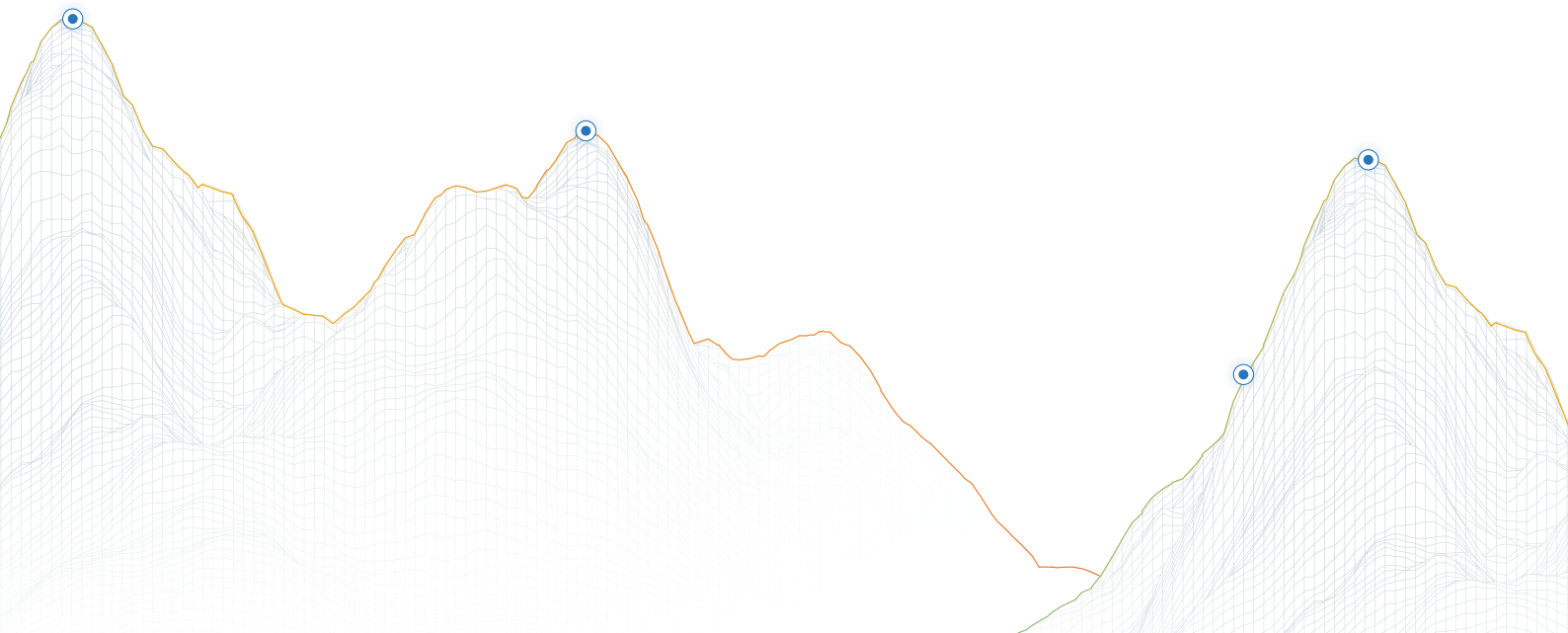
Tenable OT Security 具有弱點評估功能，有助於找出製造業企業 OT 系統、網路和應用程式內部的安全「弱點」並加以緩解。企業在主動解決弱點之下，便能夠降低網路攻擊得逞的風險。

Tenable OT Security 納入資產關鍵性評分 (ACR)，可協助資安從業人員找出作業環境的資產關鍵性。此外，也分層納入弱點優先順序評分 (VPR)，以便計算環境中所出現弱點的受攻擊程度，藉此協助資安從業人員優先修復對企業構成最大風險的弱點。這使企業能讓其資源專注於企業基礎架構中最重要的地方。企業使用風險型弱點管理方法，即可降低網路攻擊得逞的風險，並將潛在資安外洩的影響降至最低。

威脅與異常偵測

Tenable OT Security 會持續監控製造業環境中的威脅和異常活動，及早發出潛在網路安全資安事端警告。所利用的方法是偵測流量模式中發生的異常，例如大量要求資產的流量。此外，還能使用立即可用且能自訂的規則來偵測威脅，例如控制器設定偏移核准參數的狀況。

Tenable OT Security 強大的入侵偵測系統 (IDS) 引擎運用 Tenable Research 團隊所撰寫的 Suricata 規則，可找出潛藏在製造業環境中的威脅。這種偵測技術組合可讓資安從業人員找出惡意員工之中所造成的內部人員威脅、錯誤設定以及惡意軟體曝險。快速且及早偵測讓企業能夠在早期就找出資安事端或可疑的活動，對於緩解這些事端或活動所造成的影響，以及避免在未來遭受攻擊方面，更有機會迎刃而解。



裝置設定監控

隨著網路攻擊的手法和頻率與日俱增，製造業者必須保持警覺，並據以採用其安全措施。Tenable OT Security 會擷取裝置設定、韌體版本、軟體更新、詳細梯形邏輯、診斷緩衝區和標籤結構的快照，以找出基準設定的已知「良好」狀態。一旦建立基準後，Tenable OT Security 會持續追蹤控制器版本和持續性活動的完整記錄，即時監控裝置設定和行為的變更。

資安從業人員會擷取 IT 和 OT 裝置的詳細基準快照，即可找出偏差或未經授權的修改，而這些往往都代表安全風險、錯誤設定或潛在的攻擊。裝置設定監控讓企業能夠擷取及記錄設定變更和活動，藉此支援稽核與評估，若在不花費大量人工作業的情況下，這些設定變更和活動全都是難以從複雜的環境中蒐集到的資料點。此外，對於裝置層級設定的能見度，能讓資安專業人員找出可能會大幅影響製造業運作的惡意行為及錯誤設定，藉此跟上威脅態勢瞬息萬變的步伐。

Tenable 結合了上述這些功能，並且在網路安全專業知識、思維領導地位和客戶支援方面享有無與倫比的商譽，因此能夠確保讓製造業客戶不論在當下或未來都能成功防禦網路安全威脅。

關於 Tenable

Tenable® 是一家曝險管理公司。全球有 40,000 多家企業仰賴 Tenable 協助瞭解並降低網路風險。身為 Nessus® 的創造者，Tenable 拓展了本身在弱點方面的專業知識，以提供全球第一個可在任何運算平台上查看和維護任何數位資產安全的平台。在 Tenable 的客戶中，包含大約 60% 的財星 500 大企業、大約 40% 的全球 2,000 大企業以及大型政府機構。

如需深入瞭解，請前往 zh-tw.tenable.com。

總結

總結而言，在製造業中運用數位化為企業帶來顯著的效益和機會。整合數位技術並採用工業 4.0 原則在製造業運作方面造成一場革新，也因此提升了效率、生產力和彈性。製造業者經歷過許多實質性的改進，包含提高生產輸出、增加產能利用率，以及提升人工生產力。

不過，在這些優勢背後，隨之而來的是需要解決的諸多網路安全挑戰。不斷擴大的攻擊破綻、舊版系統漏洞、內部人員造成的威脅以及日新月異的威脅態勢，都會對製造業運作的安全和穩定性造成風險。由於製造業環境中所產生的獨特操作限制，以及舊版 OT 裝置的敏感本質，因此傳統的網路安全工具並不足以解決這些挑戰。

Tenable 的 OT 安全解決方案在市場上首屈一指，專為製造業者面臨的挑戰所設計，能提供深入的資產能見度、風險型弱點管理、威脅與異常偵測，以及裝置設定監控。製造業客戶可以安心仰賴 Tenable 開發尖端的網路安全產品、思維領導地位以及支援客戶克服網路安全挑戰的商譽。製造業者透過優先處理網路安全問題並建置 Tenable OT Security，就能防護其運作、緩和風險並自我定位，以在數位時代獲致成功。

資料來源

- McKinsey 於 2022 年 8 月 17 日發表之「What Are Industry 4.0, the Fourth Industrial Revolution, and 4IR?」。
- Rick Burke 及其他作者於 2021 年 9 月 16 日在 Deloitte Insights 發表之「Reshoring or localization on your mind?」。
- Deloitte 於 2022 年 8 月發表之「2023 年製造業展望」。
- IBM 於 2020 年發表之「X-Force 威脅情報索引」。
- Pingdom 團隊於 2023 年 1 月 9 日發布之「各行各業的平均停機損失」。

UNIFORCE 創泓科技

台灣區代理商 | 創泓科技股份有限公司

台北市內湖區洲子街77號10樓 | 電話：886 2 2658 3077 | 傳真：886 2 2658 3097

郵件：sales@uniforce.com.tw | www.uniforce.com.tw