Dell NativeEdge

保護：搭配零信任安全性，安心作業

表目錄

分散式環境的全方位安全性

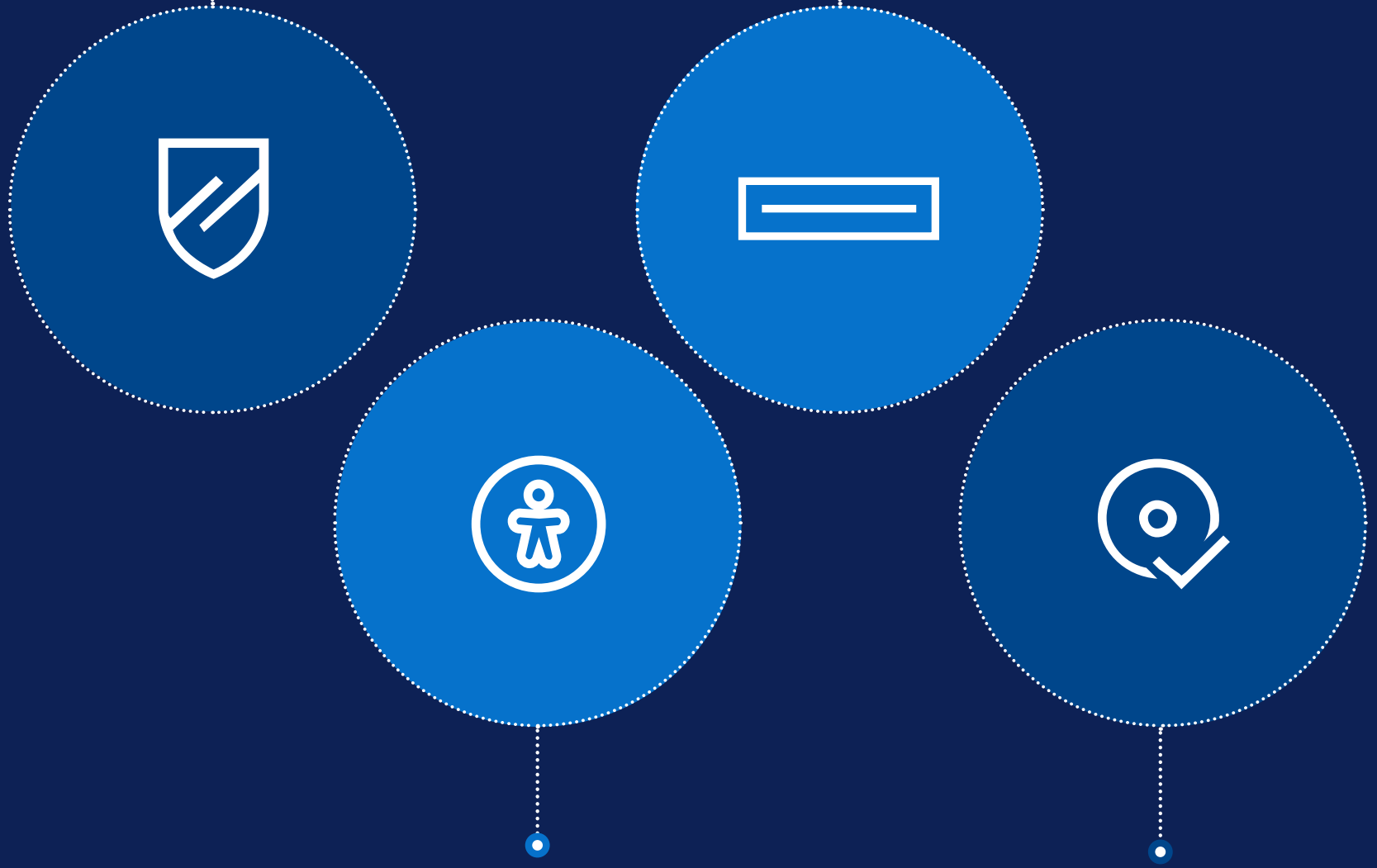
為因應瞬息萬變的客戶偏好與市場動態，企業正以前所未有的速度部署大量的新應用程式、更新及運算基礎設施。面對這股資料、基礎結構與應用程式的洪流，保護這些新技術所在的分散式環境變得越來越重要。

隨著企業擴大作業範圍，也越來越容易受到安全性風險的威脅，從實體裝置竄改到資料入侵都包含在內。此外，這些系統經常處理敏感的個人資料，使得企業在保護客戶方面肩負更重大的責任。

為確保作業安全，企業需要

確保
部署於分散式位
置之基礎結構的實體安全

偵測
裝置竄改並
修復威脅



控制
各個層級的使
用者存取權限

擴充
數千台裝置的
佈建與軟體更新作業

Dell NativeEdge

隨時隨地創新

這是一套全端、端對端的解決方案，能安全地集中管理邊緣及分散式資料中心內，各種基礎結構與應用程式的部署、協調及生命週期管理。

透過零接觸上線、零信任安全性及進階工作負載協調等功能，簡化、最佳化並保護邊緣與分散式資料中心環境。NativeEdge 運用 KVM Hypervisor 和容器執行時間，可讓組織部署和管理虛擬機器 (VM) 及容器。此平台經過最佳化，可協調 AI 工作負載與框架，在邊緣及各個分散式資料中心，實現 AI 驅動應用程式的無縫部署與管理。NativeEdge 還可依任何硬體環境進行調整，並支援各式各樣多種外型規格的選項，範圍涵蓋 Dell PowerEdge 伺服器到桌上型電腦，以及第三方基礎結構。

Dell NativeEdge 專為解決分散式環境的獨特挑戰 (如作業複雜性、擴充性與安全性) 而打造。這是專為致力於利用邊緣運算力量，同時降低成本並提升效率的現代化企業所量身定制的解決方案。

簡化
加速取得成果並
集中作業

不到
1 分鐘
即可部署基
礎結構和應用程式[1]

最佳化
實現順暢的
虛擬化和可擴充的 AI

透過
自動化邊緣
應用程式協調，
最多節省 68% 的時間[1]

保護
搭配零信任安全性
安心作業

實現全球
最安全的
邊緣作業[2]

[1] 由 Dell Technologies 委託 TechTarget 企業策略集團的技術驗證，《Dell NativeEdge - Edge Operations Software Platform》(Dell NativeEdge - 邊緣作業軟體平台)，2025 年 2 月。

[2] 根據 2025 年 5 月 Dell Technologies 內部分析結果。

Dell.com/NativeEdge

透過持續且自動化地強化基礎結構、應用程式、資料、網路及使用者的安全性，無需任何 IT 人員介入，即可保護您日益擴大的分散式作業。

Dell NativeEdge 透過以下方式保護分散式作業

確保抗竄改的硬體與軟體完整性。

在所有 NativeEdge 基礎結構上強制執行零信任。

保護邊緣、核心與雲端之間的資料及應用程式安全。

加強零信任安全性

現代企業負責管理遍布於地理分散式站點的數千個應用程式，且往往仰賴異質混合的基礎結構。這形成了複雜的技術孤島網絡，不僅管理效率低落、難以保護，且更新速度緩慢。隨著組織持續為分散式位置部署新的應用程式、感測器及裝置，潛在網路威脅的攻擊面也隨之擴大。

企業如何確保分散式資料作業的持續安全性？

Dell NativeEdge 以零信任安全性為基礎，讓您能充滿信心地作業。從裝置開啟電源的那一刻起，便利用 UEFI 安全開機與虛擬信賴平台模組 (vTPM) 等功能建立起硬體信任鏈，以確保裝置完整性。NativeEdge 內建對 GDPR 及其他全球資料主權法規的支援，讓分散式環境無後顧之憂。此方法結合零信任微分段等功能，可保護您的應用程式與資料，讓您無論在何處作業都能安全地進行創新。

零信任安全性

藉由相關的業務控制、集中式控制平面，以及明確為其運作的基礎結構，系統能監控並理解資源的所有動作，進一步強化安全性狀態。透過 NativeEdge 的零信任設計原則，企業可以高枕無憂，確信隨著分散式作業的擴展，每項連線資源的完整性都會持續經過證明與驗證。

確保供應鏈與其生命週期中的硬體完整性

以擁有全球門市或工廠據點的零售商或製造商為例，要管理並保護規格與設定檔因位置而異的多樣化硬體，變得日益困難。隨著時間推移，這些裝置未持續經過驗證，且無法在長時間範圍內確認合規性。當這些裝置的安裝涉及多方人員時，此風險將呈指數級增長。

您如何一致地保護分散式基礎結構？

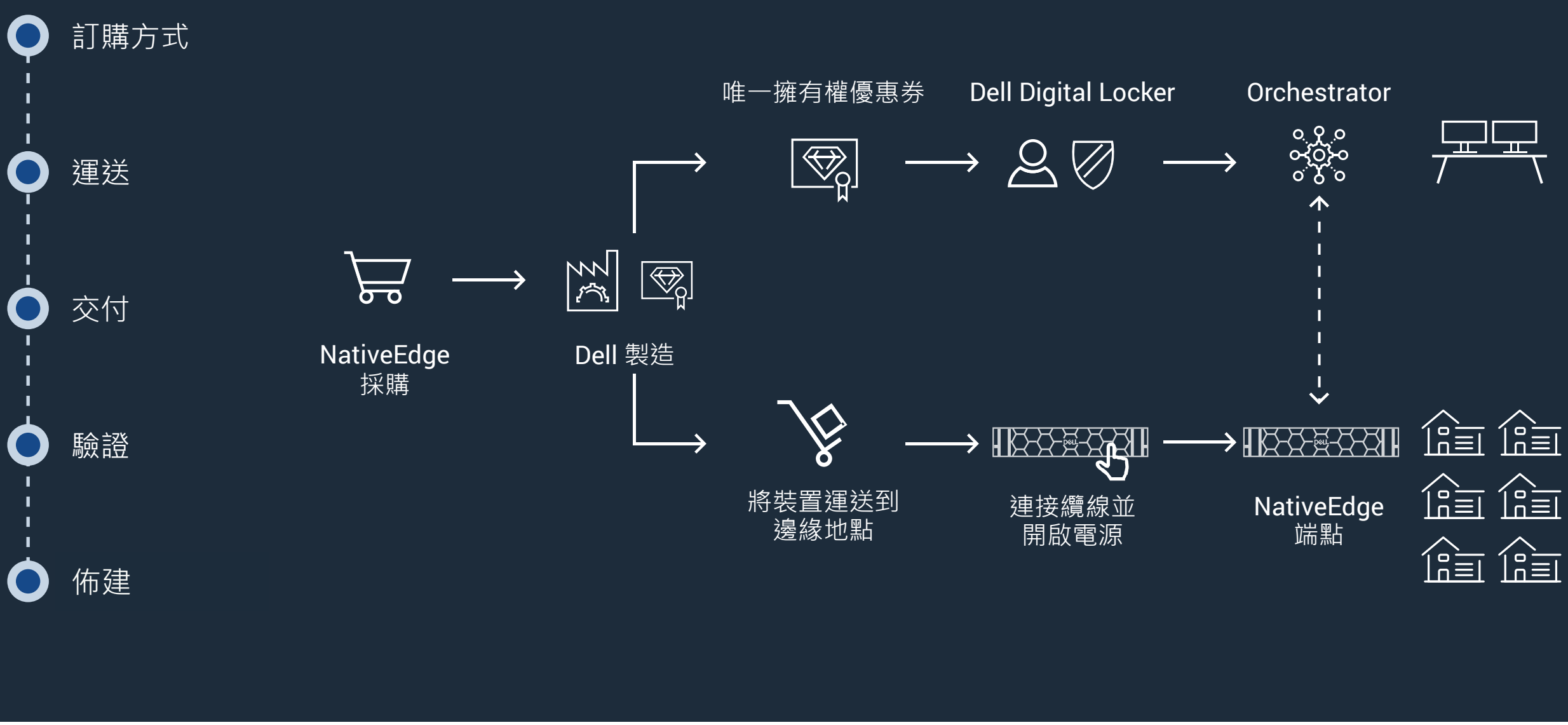
保護您的基礎結構從我們的工廠開始。NativeEdge 端點受到加密安全性與安全元件驗證 (SCV) 的保護，以確保真實性。這使得透過 FIDO 裝置上線 (FDO) 進行安全的零接觸部署流程得以實現。當裝置在任何位置開啟電源時，系統會自動驗證其完整性，無需人工介入即可建立安全的監管鏈。這讓您能擴充作業規模，並確信您的基礎結構從第一天起就安全無虞。

NativeEdge 端點已針對與 NativeEdge 的相容性進行最佳化，並在 Dell 工廠內受到加密安全性的保護。

NativeEdge 利用安全元件驗證 (SCV) 程序來確保硬體元件的真實性與完整性。NativeEdge 可透過 SCV，強制執行供應鏈完整性、元件驗證、韌體驗證、安全開機程序及密碼編譯簽章，以防範未經授權的存取或竄改。

這些裝置在進行 FIDO 裝置上線程序時，系統會自動認證其完整性，確保從 Dell 工廠製造到部署站點接收與安裝的這段期間皆安全無虞。若硬體遭到任何方式的竄改，平台會自動將其隔離，保護作業免受惡意元素的影響。

安全裝置上線和零信任架構

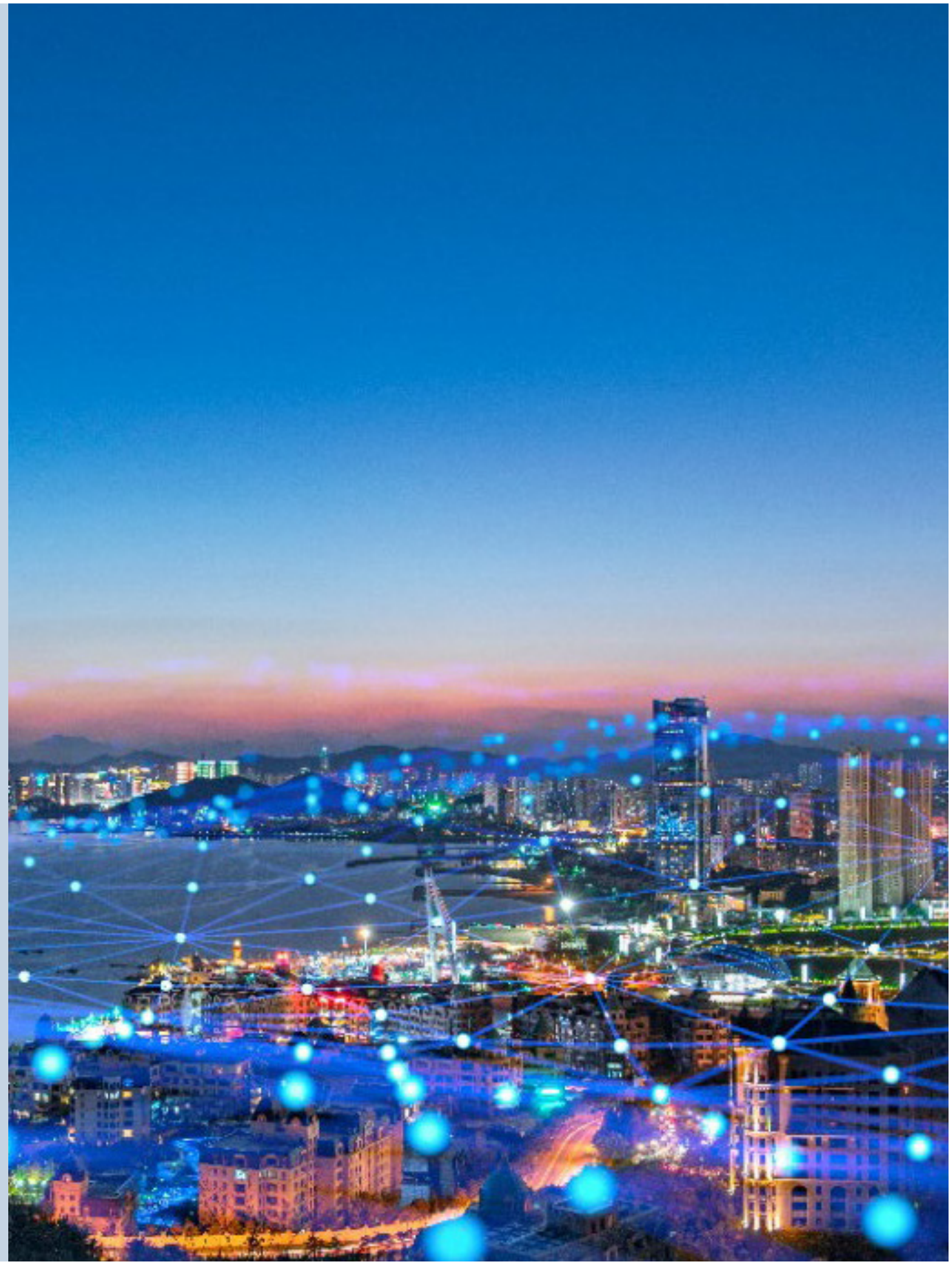


強化從邊緣到雲端的資料和應用程式

試以一家全球零售商為例。零售環境的分散與分佈特性，意味著存取應用程式與工作負載的使用者身分可能無法受到例行性的驗證。即使有驗證，通常也僅限於該環境本地，無法從集中檢視與稽核。

此外，零售商鮮少具備已部署應用程式軟體供應鏈的可見度。這些通常由管理式服務供應商 (MSP) 處理，且可能缺乏針對這些應用程式真實性的可見度自動檢查。這些應用程式通常最初由相同的 MSP 進行設定，隨著時間推移，可能會發生組態漂移。因此，利害關係人無法判斷應用程式是否符合安全性原則。

在製造商的案例中，作業技術 (OT) 團隊通常會執行各式各樣的應用程式工作負載。其中部分應用程式會與 PLC 等設備對接，且屬於缺乏內部可見度的專屬應用程式。



IT 網路功能無法向下延伸至邏輯上分離的 OT 網路，結果為何？製造商 OT 網路內部的基礎結構與應用程式工作負載，無法取得促進安全 OT 環境所需的網路安全控制層級。各行各業普遍都有類似的應用程式與資料安全挑戰。

Dell NativeEdge 協助組織保護資料管道，範圍涵蓋從資料來源到在本機或雲端執行的應用程式。它結合了進階安全措施，例如加密、使用者存取控制、應用程式藍圖目錄、網路分段及安全性協調流程。NativeEdge 亦利用遙測與分析功能，主動評估分散式據點的安全性狀態，無需仰賴具備稽核能力的專家親臨每個現場。

進階的安全性措施可確保作業具備韌性

使用者存取控制

NativeEdge 提供角色型存取控制 (RBAC) 功能，根據使用者的角色與職責劃分存取層級。針對裝置與已部署應用程式工作負載的使用者，系統會針對每個存取工作階段進行驗證，並透過身分與存取管理，以集中且可見的方式進行證明。

網路分段

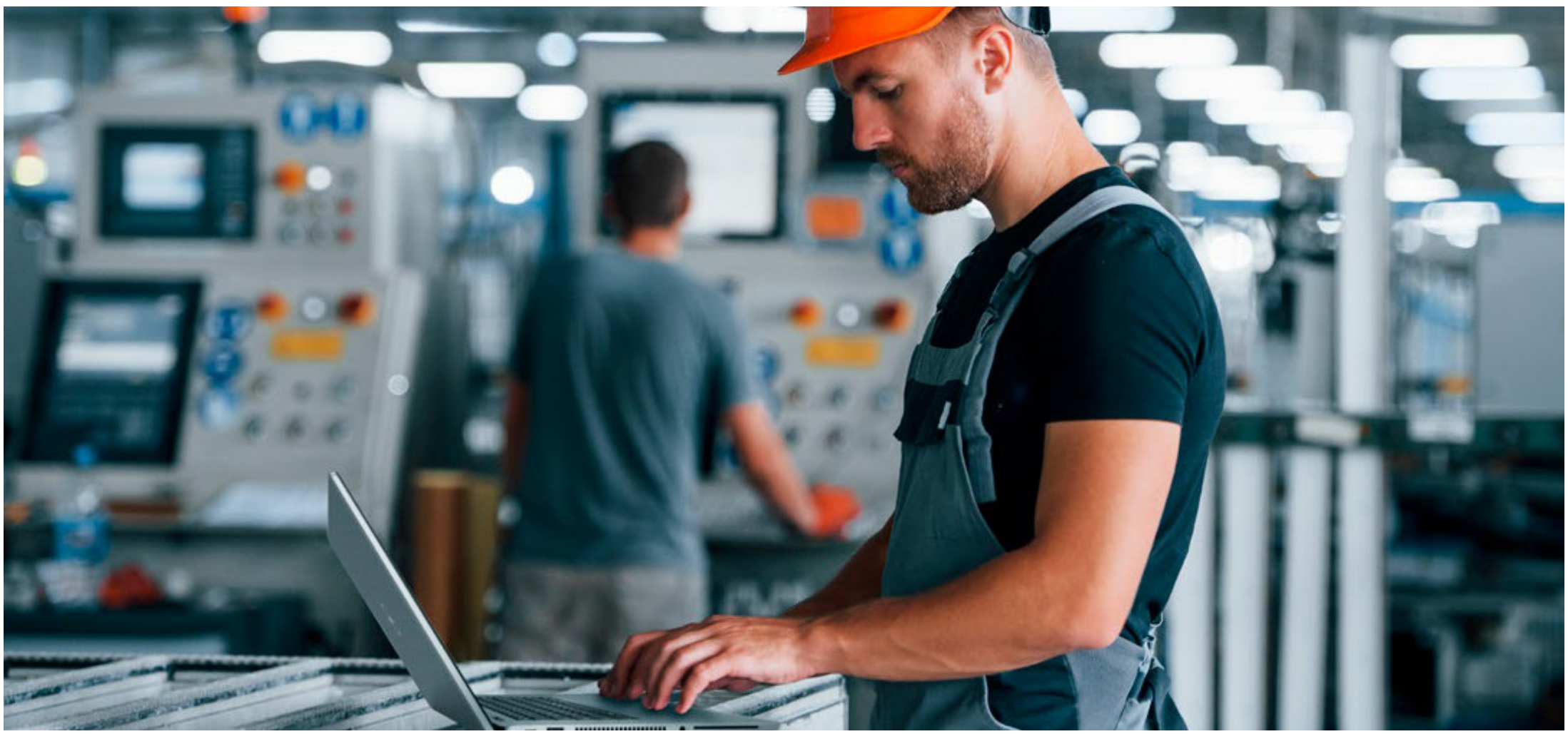
針對應用程式進行網路微分段，讓開發與管理針對這些應用程式的原則變得更容易，進而提升其安全性。此方法可減輕潛在入侵風險，並防止威脅在虛擬化環境內橫向移動。

應用程式藍圖目錄

NativeEdge 旨在提升應用程式的安全性。這一點始於安全的軟體供應鏈，該供應鏈仰賴「目錄」並透過藍圖來部署您的應用程式。「目錄」是藍圖的集合，包含來自獨立軟體廠商 (ISV) 的應用程式，或由企業開發且經 Dell 預先驗證的藍圖，旨在維護安全的軟體供應鏈。這些藍圖採用 TOSCA 標準與 YAML 格式，可同時將應用程式及 AI 框架自動部署至眾多邊緣裝置。NativeEdge 讓您能以精細的層級，針對已部署的應用程式設定主動式安全控制，確保應用程式部署一致並符合您的安全性原則。最後，應用程式工作負載可做為 VM 與容器，在 NativeEdge 端點或多雲環境中執行，並由 NativeEdge 集中管理。

資料加密與保護

無論您的資料位於何處 (待用中、傳輸中或使用中) NativeEdge 都能加以保護，防範資料外洩與未經授權的存取。NativeEdge 提供強大的待用資料加密 (DARE) 功能，符合聯邦合規標準，確保儲存的資料經過加密，並保護其免於實體竊盜或竄改。NativeEdge 採用零信任安全原則管理每一項資料資源，強制執行嚴格的存取控制，並持續證明與驗證該存取控制。這不僅可以保護企業應用程式的資料完整性，也能增強所有業務利害關係人的信心。



安全性協調

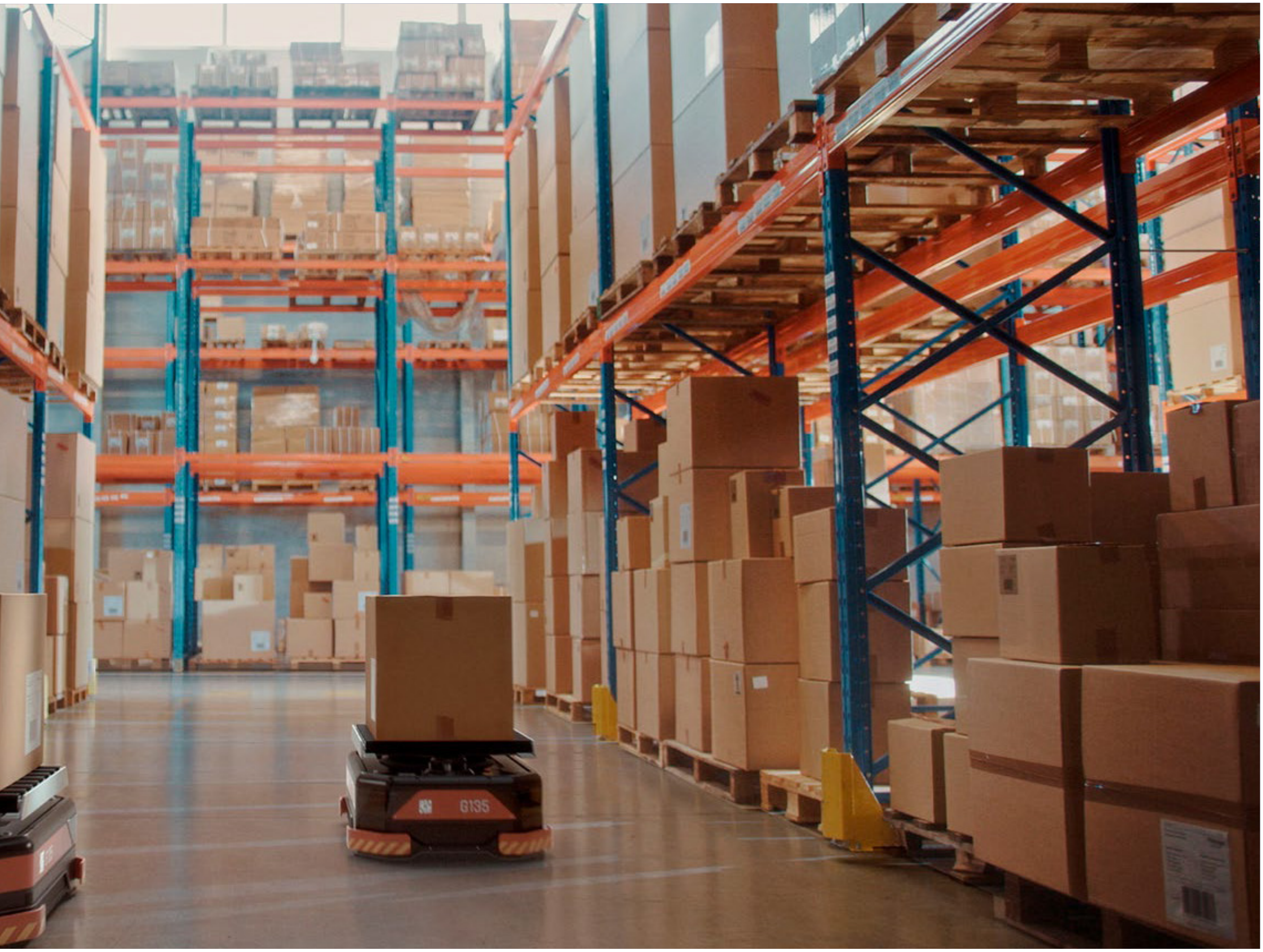
未經授權的動作或事件往往在不知不覺中發生，且經常未經過修復。由於手動程序之故，這不僅帶來風險，且安全性維護往往因優先處理高重要性業務任務而受忽略。此外，身分識別存取管理 (IAM)、角色型存取控制 (RBAC) 及控制平面之間的 IT 整合存在差異。

這導致安全性協調脫節，通常淪為每個站點各自為政的管理模式。在許多 OT 案例中，這些裝置處於機器對機器 (M2M) 環境，缺乏使用者感知能力。因此，集中式協調對這些環境至關重要。

NativeEdge 可確保整個邊緣資產擁有一致的安全性協調。它能根據邊緣環境中發生的動作與事件總合，提供您安全性態勢的統一檢視，實現集中式驗證並在所有站點強制執行一致的原則。它利用 IAM 與 RBAC 功能，依循最小權限原則實現平台的安全管理，進而提供企業所需的細緻度。NativeEdge 亦透過自動化記錄與組態管理，簡化 GDPR、PCI 及 HIPAA 等法規的遵循工作，並具備整合治理、風險與合規 (GRC)/安全維運 (SecOps) 規則的能力，協助您在任何環境中皆能充滿自信地作業。

遙測與分析

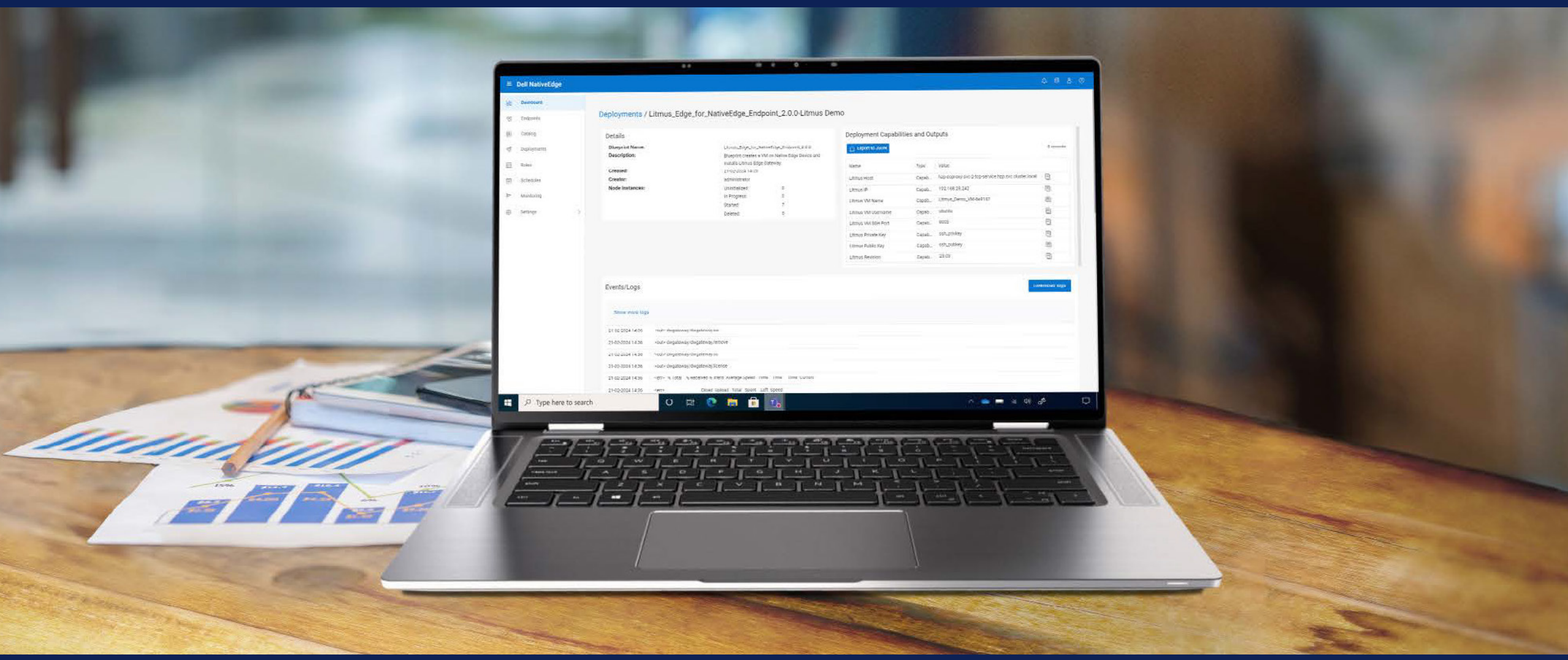
NativeEdge 仰賴來自硬體與作業環境的遙測資料，依據定義的合規標準持續執行安全性評估。這些資料可用於偵測組態漂移、組態設定錯誤，以及判定是否有安全性更新的需求。



保護邊緣資產

Dell NativeEdge 透過零信任安全原則保護您的邊緣資產，其中包含以 FIDO 為基礎的安全裝置上線功能，並結合經強化且的安全 NativeEdge 作業系統。有了 Dell NativeEdge，您可以高枕無憂，確信您的基礎結構、使用者、網路、應用程式及資料，在各個分散式據點皆會持續經過證明與驗證。

隨時隨地創新



DELL Technologies

如需深入了解，請前往 **Dell.com/NativeEdge**