Dell NativeEdge

Protezione: massima tranquillità con la sicurezza Zero Trust

Tabella.

Sommario

Sicurezza in tutti gli ambienti distribuiti

Per rispondere alle preferenze dei clienti in rapida evoluzione e alle dinamiche di mercato, le organizzazioni stanno implementando nuove applicazioni, aggiornamenti e infrastrutture informatiche a un volume e una velocità senza precedenti. Questo flusso massiccio di dati, infrastrutture e applicazioni rende sempre più cruciale proteggere gli ambienti distribuiti in cui risiedono queste nuove tecnologie.

Con l'espansione delle operazioni, le aziende diventano sempre più vulnerabili ai rischi per la sicurezza, dalla manomissione fisica dei dispositivi agli attacchi informatici sui dati. Inoltre, questi sistemi gestiscono spesso dati personali sensibili, aumentando la responsabilità delle imprese nella protezione dei propri clienti.

Per proteggere le operazioni, le aziende devono

Garantire
la sicurezza fisica dell'infrastruttura implementata in sedi distribuite

Rilevare
attività di manomissione dei dispositivi e correggere minacce

Controllare
l'accesso degli utenti a ogni livello

Dimensionare
il provisioning e gli aggiornamenti software su migliaia di dispositivi

Dell NativeEdge

Innovate ovunque

Una soluzione full-stack end-to-end che centralizza in modo sicuro l'implementazione, l'orchestration e la gestione del ciclo di vita di infrastrutture e applicazioni diversificate all'edge e nei data center distribuiti.

Semplifica, ottimizza e proteggi gli ambienti edge e dei data center distribuiti con funzionalità come onboarding zero-touch, sicurezza Zero Trust e orchestration avanzata dei carichi di lavoro. NativeEdge sfrutta un hypervisor KVM e il runtime dei container, consentendo alle organizzazioni di implementare e gestire sia macchine virtuali che container. È ottimizzato per l'orchestration dei framework e dei carichi di lavoro di AI per l'implementazione e la gestione delle applicazioni basate sull'AI all'edge e nei data center distribuiti. NativeEdge si adatta anche a qualsiasi ambiente hardware, supportando un'ampia gamma di opzioni in vari fattori di forma, dai server Dell PowerEdge ai desktop, nonché un'infrastruttura di terze parti.

Dell NativeEdge è progettato appositamente per affrontare le sfide specifiche degli ambienti distribuiti: complessità operativa, scalabilità e sicurezza. È una soluzione pensata per le organizzazioni moderne che vogliono sfruttare appieno la potenza dell'edge computing, riducendo i costi e migliorando l'efficienza.

Semplificazione

Accelerazione dei risultati e centralizzazione delle operazioni

Meno di
1 minuto
per l'implementazione dell'infrastruttura e delle applicazioni[1]

Optimize

Fluidità delle operazioni con virtualizzazione e AI scalabile

Fino al
68%
di tempo risparmiato grazie all'automazione dell'orchestration delle applicazioni edge[1]

Protezione

Operazioni in tutta tranquillità grazie alla sicurezza Zero Trust

Le operazioni edge
più sicure
al mondo[2]

[1] Convalida tecnica di Enterprise Strategy Group by TechTarget commissionata da Dell Technologies, "Dell NativeEdge Edge Operations Software Platform", febbraio 2025.

[2] Dati basati su un'analisi interna Dell Technologies, maggio 2025.

Dell.com/NativeEdge

Proteggi le tue operazioni distribuite in espansione rafforzando in modo persistente e automatico la sicurezza di infrastruttura, applicazioni, dati, rete e utenti, senza alcun intervento da parte del team IT.

Dell NativeEdge protegge le operazioni distribuite:

Consolidamento della sicurezza Zero Trust

Le aziende moderne sono responsabili della gestione di migliaia di applicazioni distribuite su siti geograficamente lontani e spesso si affidano a un'infrastruttura eterogenea. Questo crea una rete complessa di silos tecnologici inefficienti da gestire, difficili da proteggere e lenti da aggiornare. Man mano che le organizzazioni continuano a implementare nuovi sensori, dispositivi e applicazioni nelle sedi distribuite, cresce anche la superficie di attacco per potenziali minacce informatiche.

In che modo le aziende possono garantire la sicurezza continua delle operazioni sui dati distribuiti?

Dell NativeEdge consente di operare in tutta tranquillità grazie a un approccio basato sulla sicurezza Zero Trust. Dal momento in cui un dispositivo viene acceso, viene stabilita una catena di attendibilità radicata nell'hardware, utilizzando funzionalità come UEFI Secure Boot e un Trusted Platform Module virtuale (vTPM) per garantire l'integrità del dispositivo. Con il supporto integrato per il GDPR e altre normative globali sulla sovranità dei dati, NativeEdge offre tranquillità negli ambienti distribuiti. Questo approccio, combinato con funzionalità come la microsegmentazione Zero Trust, protegge applicazioni e dati, consentendoti di innovare in sicurezza, ovunque.

Sicurezza Zero-Trust

Il profilo di sicurezza è ulteriormente rafforzato dal monitoraggio e dalla comprensione di tutte le azioni delle risorse, grazie ai controlli aziendali pertinenti, a un piano di controllo centralizzato e a un'infrastruttura che opera che opera esplicitamente a loro favore. Grazie ai principi di progettazione Zero Trust di NativeEdge, le aziende possono avere la certezza che, con l'espansione delle operazioni distribuite, l'integrità di ogni risorsa connessa venga continuamente verificata e attestata.

Integrità hardware garantita nell'intera supply chain e per tutto il ciclo di vita

Prendendo come esempio un rivenditore o un produttore con sedi di negozi o stabilimenti distribuiti a livello globale, diventa sempre più difficile gestire e proteggere hardware eterogeneo, che presenta specifiche e profili diversi a seconda della sede. Col tempo, questi dispositivi non vengono continuamente attestati e la conformità non può essere verificata su larga scala temporale. Questo rischio aumenta in modo esponenziale quando più soggetti sono coinvolti nell'installazione di tali dispositivi.

Come proteggere in modo coerente l'infrastruttura distribuita?

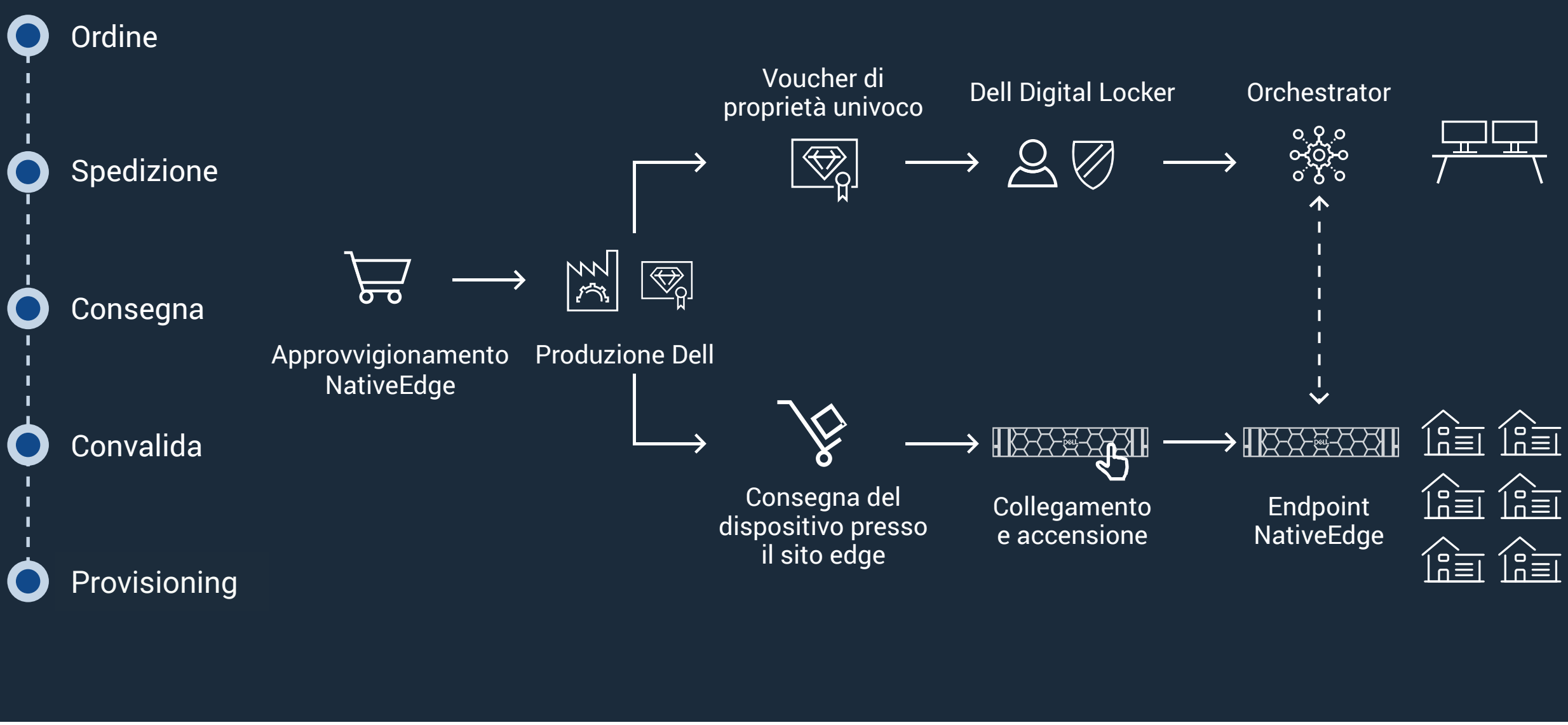
La protezione della tua infrastruttura inizia già in fabbrica.
Gli endpoint NativeEdge sono protetti con sicurezza crittografica e Secured Component Verification (SCV) per garantirne l'autenticità. Ciò consente un processo di deployment zero-touch sicuro tramite FIDO Device Onboarding (FDO). Quando un dispositivo viene acceso in qualsiasi sede, la sua integrità viene automaticamente verificata, stabilendo una catena di custodia sicura senza intervento manuale. Questo permette di dimensionare le operazioni sapendo che l'infrastruttura è sicura fin dal primo giorno.

Gli endpoint NativeEdge sono ottimizzati per la compatibilità con NativeEdge e protetti con sicurezza crittografica la fabbrica Dell.

NativeEdge sfrutta il processo di Secured Component Verification (SCV) per garantire l'autenticità e l'integrità dei componenti hardware. Attraverso SCV, NativeEdge assicura l'integrità della supply chain, la verifica dei componenti, la convalida del firmware, i processi di avvio protetto e le firme crittografiche, proteggendo dai tentativi di accesso non autorizzato o manomissione.

Quando questi dispositivi attraversano il processo di onboarding basato su FIDO, la loro integrità viene automaticamente certificata, garantendo sicurezza dalla produzione nella fabbrica Dell fino alla ricezione e all'installazione nel sito di implementazione. In caso di manomissione hardware, la piattaforma isola automaticamente i dispositivi compromessi, proteggendo le operazioni da elementi non autorizzati.

Onboarding sicuro dei dispositivi e framework Zero Trust

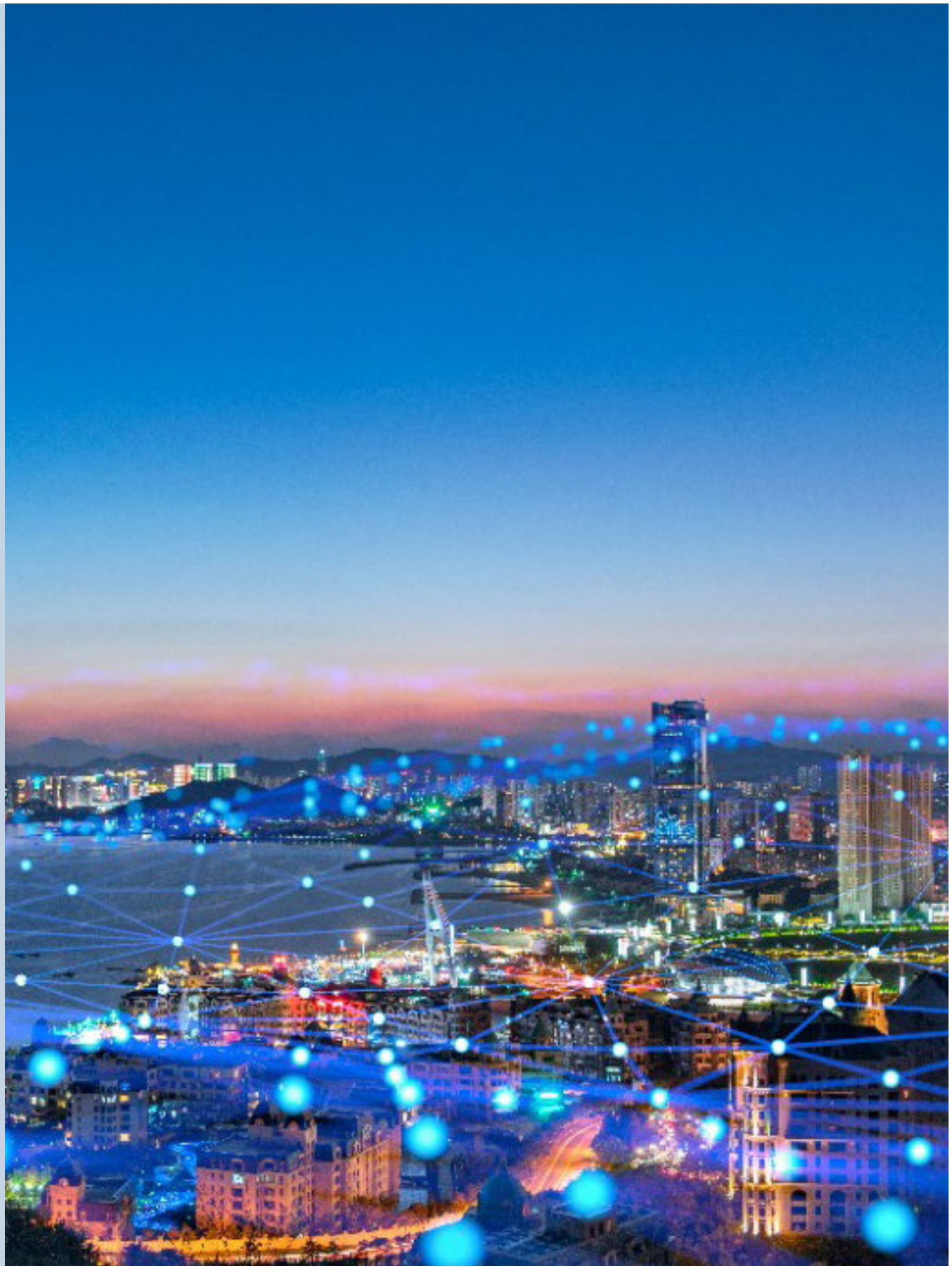


Dati e applicazioni rafforzati, dall'edge al cloud

Prendiamo come esempio un rivenditore globale. La natura eterogenea e distribuita degli ambienti retail implica che le identità degli utenti che accedono ad applicazioni e carichi di lavoro potrebbero non essere verificate in modo sistematico. E quando lo sono, la verifica avviene solo a livello locale e non è visibile né verificabile centralmente.

Inoltre, i rivenditori hanno spesso scarsa visibilità sulla supply chain software delle applicazioni implementate. Queste sono spesso gestite da Managed Service Provider (MSP) e potrebbero non essere previsti controlli automatizzati visibili sulla correttezza di tali app. Spesso le applicazioni vengono configurate inizialmente dagli stessi MSP, con il rischio di una deviazione della configurazione nel tempo. Di conseguenza, le entità interessate non sono in grado di determinare la conformità delle applicazioni alle policy di sicurezza.

Nel caso dei produttori, il team di Operations Technology (OT) generalmente gestisce un insieme eterogeneo di carichi di lavoro applicativi. Alcune di queste applicazioni interagiscono con dispositivi come PLC e sono applicazioni proprietarie senza visibilità interna.



Le capacità della rete IT non si estendono alla rete OT, che è logicamente separata. Il risultato? L'infrastruttura e i carichi di lavoro applicativi all'interno delle reti OT dei produttori non dispongono del livello di controlli di sicurezza di rete necessario per garantire un ambiente OT sicuro. Sfide simili relative alla sicurezza di applicazioni e dati sono comuni in tutti i settori.

Dell NativeEdge aiuta le organizzazioni a proteggere la pipeline di dati, dalle origini dati fino alle applicazioni eseguite localmente o nel cloud. Combina misure di sicurezza avanzate come crittografia, controllo degli accessi degli utenti, catalogo di blueprint applicativi, segmentazione della rete e orchestration della sicurezza. NativeEdge utilizza inoltre telemetria e analisi per valutare in modo proattivo il profilo di sicurezza delle sedi distribuite, senza dover contare su esperti con capacità di audit che visitino ogni sito.

Misure di sicurezza avanzate

Le misure di sicurezza avanzate assicurano operazioni resilienti

Controllo degli accessi degli utenti

NativeEdge fornisce il controllo degli accessi basato sui ruoli (RBAC) per analizzare i livelli di accesso in base ai ruoli e alle responsabilità di un utente. Gli utenti dei dispositivi e dei carichi di lavoro delle applicazioni implementati vengono verificati a ogni sessione di accesso e attestati in modo centralizzato e visibile tramite la gestione delle identità e degli accessi.

Segmentazione della rete

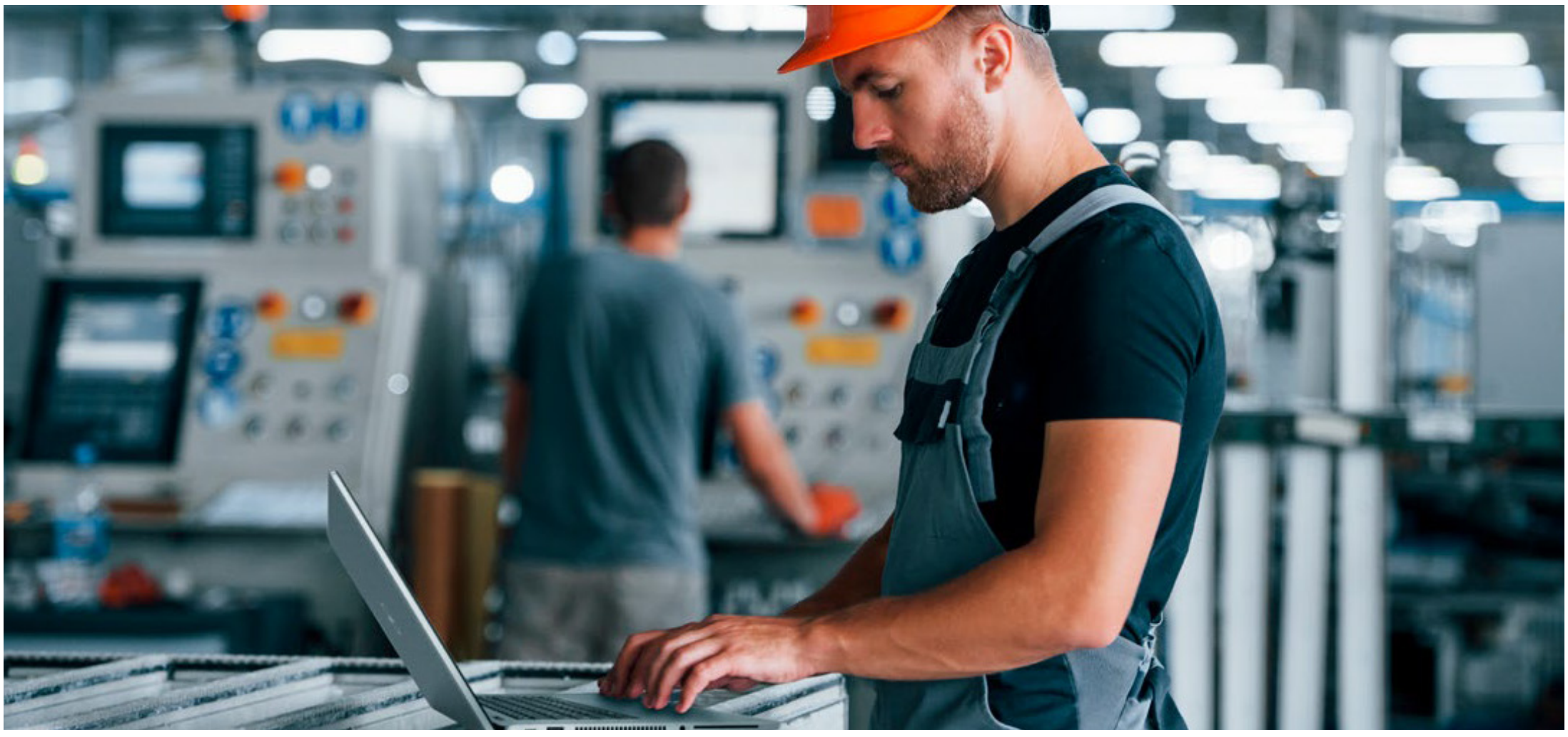
La microsegmentazione della rete per le applicazioni semplifica lo sviluppo e la gestione delle policy destinate a queste applicazioni, aumentando la loro sicurezza. Questo approccio riduce i rischi di potenziali violazioni e il movimento laterale delle minacce all'interno di ambienti virtualizzati.

Catalogo di blueprint delle applicazioni

NativeEdge è progettato per rendere le applicazioni più sicure. Tutto inizia con una supply chain software sicura, basata su un catalogo che consente di implementare le applicazioni tramite blueprint. Il catalogo è una raccolta di blueprint per implementare applicazioni da fornitori di software indipendenti (ISV) o blueprint preconvalidati da Dell e sviluppati dalle aziende, garantendo così una supply chain software sicura. Questi blueprint, basati sullo standard TOSCA e sul formato YAML, automatizzano l'implementazione delle applicazioni e dei framework AI su numerosi dispositivi edge contemporaneamente. NativeEdge consente di impostare controlli di sicurezza proattivi per le applicazioni implementate a livello granulare e garantisce che le applicazioni siano implementate in modo coerente, in linea con le policy di sicurezza. Infine, i carichi di lavoro applicativi possono essere eseguiti su endpoint NativeEdge o in un ambiente multicloud come macchine virtuali e container, gestiti centralmente da NativeEdge.

Crittografia e protezione dei dati

NativeEdge protegge i dati ovunque si trovino (inattivi, in transito e in uso) da violazioni e accessi non autorizzati. NativeEdge fornisce un modello DARE affidabile, che soddisfa gli standard di conformità federali, garantendo che i dati archiviati siano cifrati e protetti contro furti o manomissioni fisiche. NativeEdge gestisce ogni risorsa dati secondo i principi della sicurezza Zero Trust, applicando controlli di accesso rigorosi e attestando e verificando continuamente tali accessi. Questo non solo protegge l'integrità dei dati per le applicazioni aziendali, ma aumenta anche la fiducia di tutte le entità interessate dell'azienda.

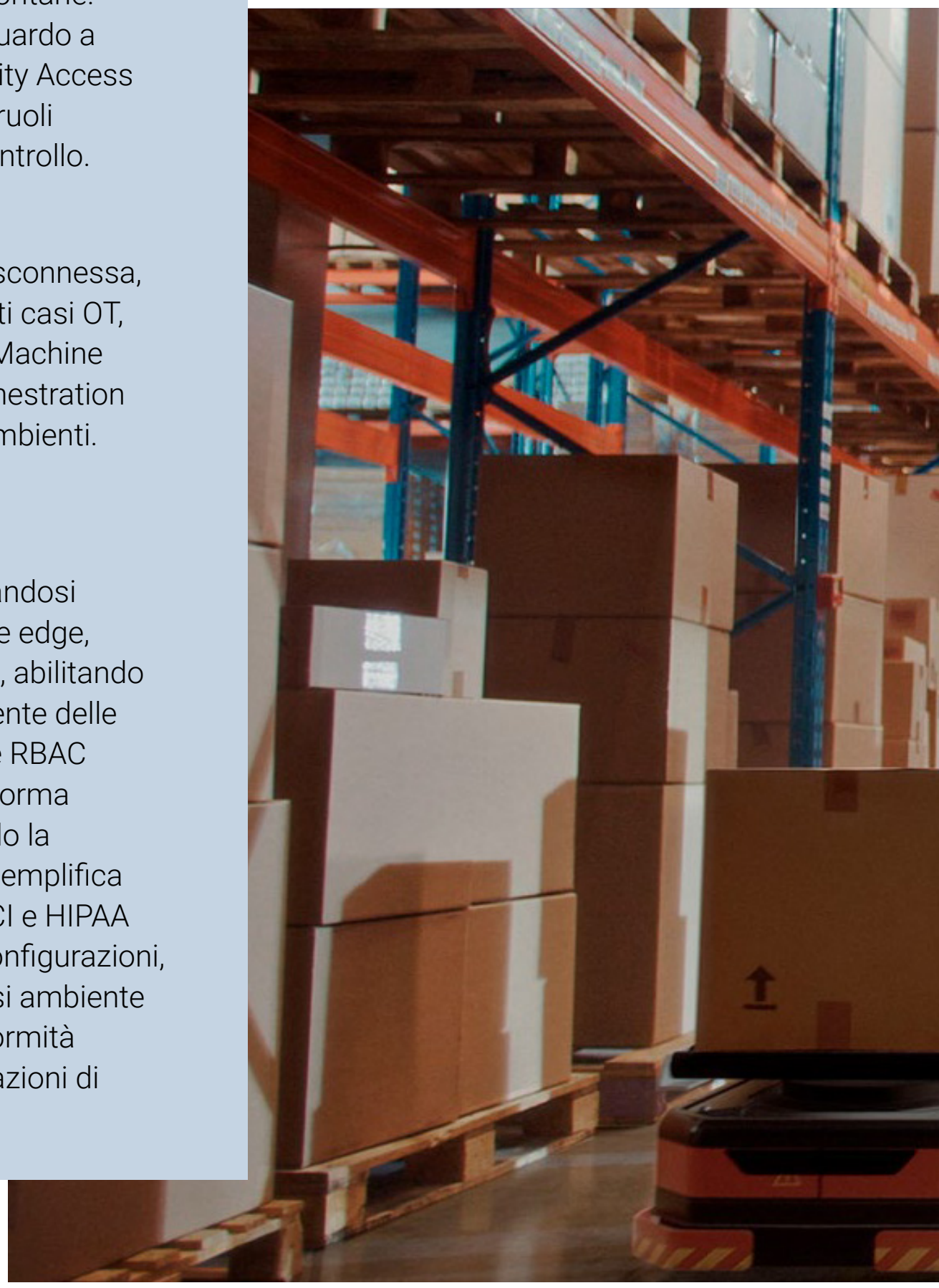


Orchestration della sicurezza

Le azioni o gli eventi non autorizzati spesso passano inosservati e raramente vengono corretti. Questo genera rischi legati a processi manuali, che spesso vengono messi in secondo piano rispetto ad attività aziendali prioritarie. Inoltre, esistono variazioni nell'integrazione IT riguardo a gestione delle identità e degli accessi (IAM, Identity Access Management)/controllo degli accessi basato su ruoli (RBAC, Role-Based Access Control) e piano di controllo.

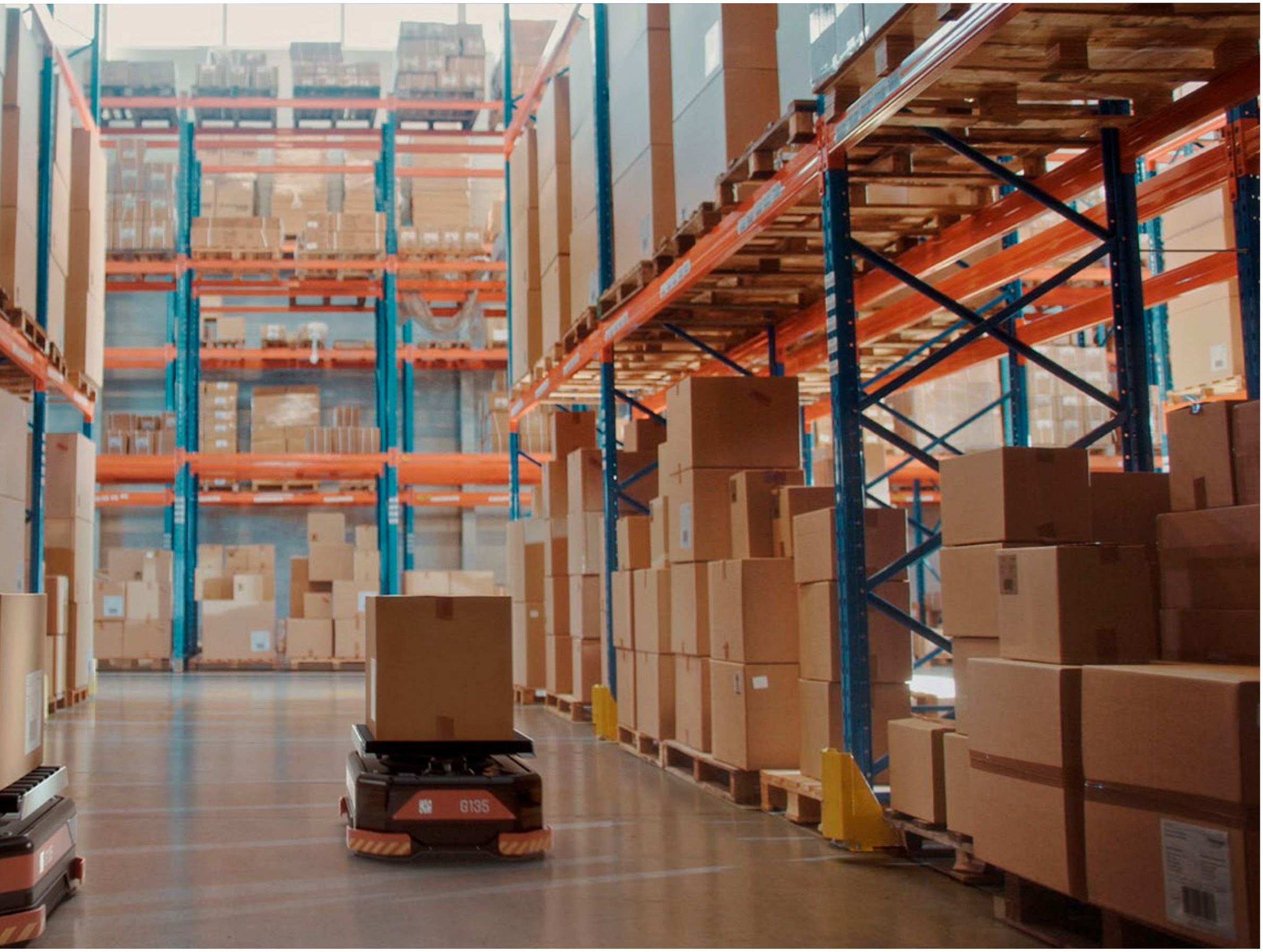
Ciò comporta un'orchestration della sicurezza disconnessa, spesso gestita singolarmente in ogni sito. In molti casi OT, i dispositivi operano in un ambiente Machine-to-Machine (M2M) senza consapevolezza dell'utente. Un'orchestration centralizzata è quindi fondamentale per questi ambienti.

NativeEdge garantisce un'orchestration della sicurezza coerente in tutto l'ambiente edge. Basandosi sull'aggregazione di azioni ed eventi nell'ambiente edge, offre una visione unificata del profilo di sicurezza, abilitando autenticazione centralizzata e applicazione coerente delle policy in tutti i siti. Utilizza le funzionalità di IAM e RBAC per consentire una gestione protetta della piattaforma secondo il principio del privilegio minimo, offrendo la granularità necessaria alle aziende. NativeEdge semplifica anche la conformità a normative come GDPR, PCI e HIPAA automatizzando registrazione e gestione delle configurazioni, permettendo di operare con sicurezza in qualsiasi ambiente e integrando regole da governance, rischi e conformità (GRC, Governance, Risk and Compliance) e operazioni di sicurezza (SecOps, Security Operations).



Telemetria e analisi

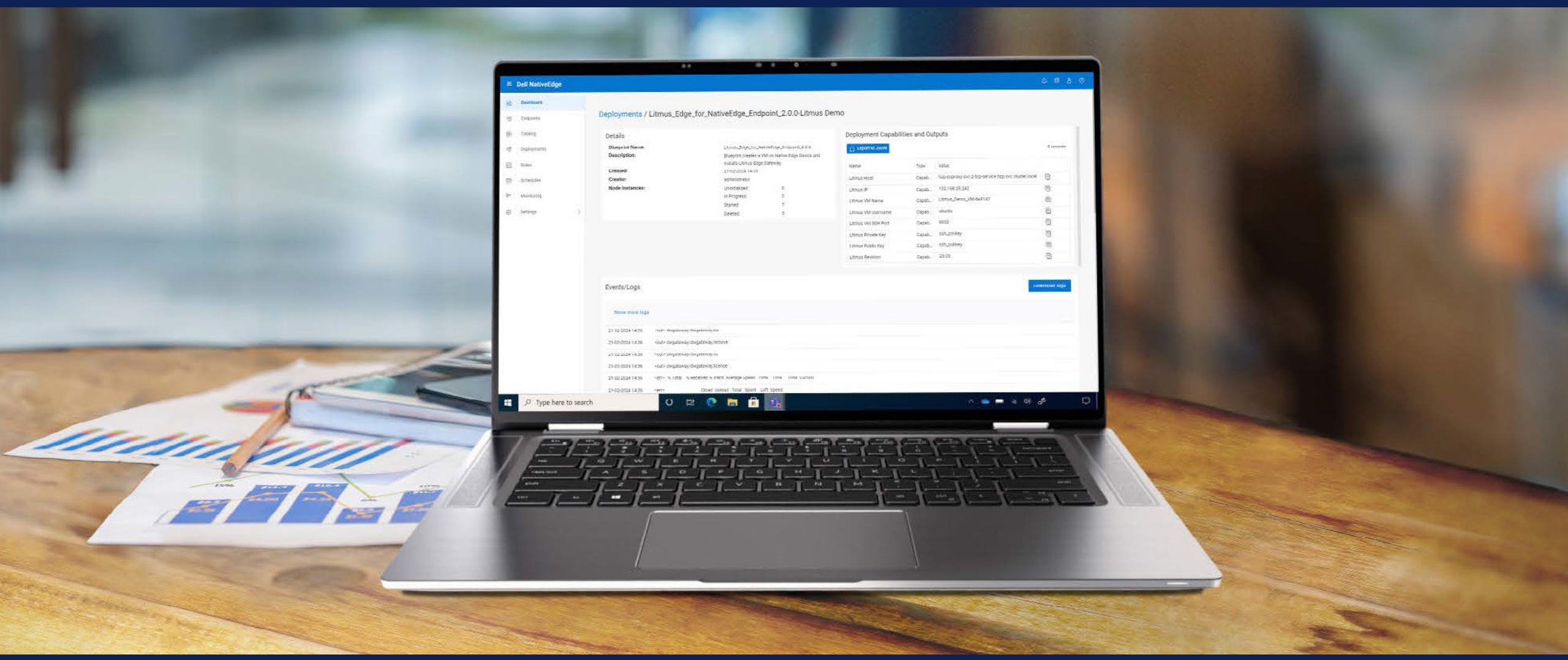
NativeEdge esegue continuamente valutazioni di sicurezza in linea con gli standard di conformità definiti, sfruttando la telemetria proveniente dall'hardware e dall'ambiente operativo. Questi dati vengono utilizzati per rilevare deviazioni dalle configurazioni, errori di configurazione e la necessità di aggiornamenti di sicurezza.



Protezione dell'ambiente edge

Dell NativeEdge protegge l'ambiente edge con principi di sicurezza Zero Trust, tra cui l'onboarding sicuro dei dispositivi basato su FIDO, abbinato a un sistema operativo NativeEdge rinforzato e sicuro. Con Dell NativeEdge hai la certezza che l'infrastruttura, gli utenti, la rete, le applicazioni e i dati vengano continuamente attestati e convalidati in tutte le sedi distribuite.

Innovate ovunque



DELL Technologies

Scopri di più su **Dell.com/NativeEdge**