Dell NativeEdge

Schützen: Zuverlässiger Betrieb mit Zero-Trust-Sicherheit

Inhalts-

Inhalt

Sicherheit in verteilten Umgebungen

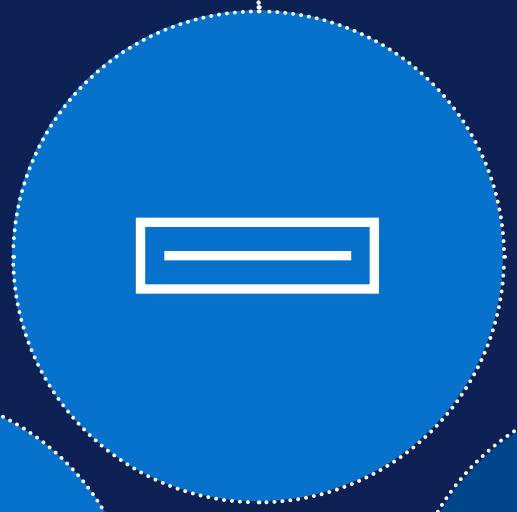
Um den sich schnell ändernden Kundenpräferenzen und der Marktdynamik gerecht zu werden, stellen Unternehmen neue Anwendungen, Updates und Compute-Infrastruktur in einer bisher unerreichten Menge und Geschwindigkeit bereit. Diese Flut an Daten, Infrastruktur und Anwendungen macht es zunehmend kritisch, die verteilten Umgebungen zu sichern, in denen sich diese neuen Technologien zum Einsatz kommen.

Wenn Unternehmen ihren Betrieb erweitern, werden sie anfälliger für Sicherheitsrisiken, die von Gerätemanipulationen bis hin zu Daten-Hacking reichen. Darüber hinaus verarbeiten diese Systeme häufig sensible personenbezogene Daten, sodass Unternehmen mehr Verantwortung für den Schutz ihrer Kunden übernehmen.

Um den Betrieb zu sichern, müssen Unternehmen:

die
physische Sicherheit der
an verteilten Standorten bereitgestellten
Infrastruktur gewährleisten

Gerätemanipulationen
erkennen
und Bedrohungen beheben



den
Nutzerzugriff auf jeder
Ebene kontrollieren

Berreitstellungen
und Softwareupdates auf
Tausenden von Geräten skalieren

Dell NativeEdge

Schaffen Sie Innovationen, wo auch immer Sie arbeiten

Eine durchgängige Full-Stack-Lösung, die die Bereitstellung, Orchestrierung und das Lebenszyklusmanagement verschiedener Infrastrukturen und Anwendungen am Edge und in verteilten Rechenzentren sicher zentralisiert.

Vereinfachen, optimieren und schützen Sie Edge- und verteilte Rechenzentrumsumgebungen mit Funktionen wie Zero-Touch-Onboarding, ZeroTrust-Sicherheit und erweiterter Workload-Orchestrierung. NativeEdge nutzt einen KVM-Hypervisor und eine Container-Laufzeit, sodass Unternehmen sowohl virtuelle Maschinen (VM) als auch Container bereitstellen und managen können. Die Lösung ist für die Orchestrierung von KI-Workloads und Frameworks optimiert und ermöglicht so eine nahtlose Bereitstellung und Verwaltung von KI-gesteuerten Anwendungen am Edge und in verteilten Rechenzentren. NativeEdge kann außerdem an beliebige Hardwareumgebungen angepasst werden und unterstützt eine Vielzahl von Optionen in verschiedenen Formfaktoren – von Dell PowerEdge-Servern über Desktops bis hin zu Infrastruktur von Drittanbietern.

Dell NativeEdge wurde speziell entwickelt, um die einzigartigen Herausforderungen verteilter Umgebungen wie betriebliche Komplexität, Skalierbarkeit und Sicherheit anzugehen. Es handelt sich um eine Lösung, die auf moderne Unternehmen zugeschnitten ist, die sich darauf konzentrieren, die Leistungsfähigkeit von Edge Computing zu nutzen und gleichzeitig Kosten zu senken und die Effizienz zu verbessern.

Vereinfachen
Schnellere Ergebnisse und Zentralisierung des Betriebs

Weniger als
1 Minute
bis zur Bereitstellung von Infrastruktur und Anwendungen[1]

Optimierung
Nahtlose Virtualisierung und skalierbare KI

Zeitersparnis von bis zu
68 %
durch die Automatisierung der Anwendungsorchestrierung am Edge.[1]

Schutz
Zuverlässiger Betrieb mit Zero-Trust-Sicherheit

Realisierung der weltweit
sichersten
Edge-Prozesse[2]

[1] Technische Validierung durch Enterprise Strategy Group von TechTarget im Auftrag von Dell Technologies, „Dell NativeEdge – eine Edge-Betriebssoftwareplattform", Februar 2025.

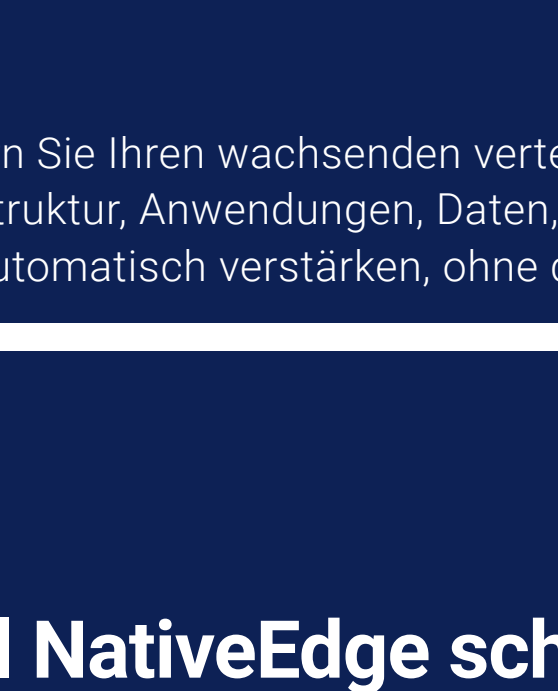
[2] Basierend auf einer internen Analyse von Dell Technologies, Mai 2025.

Dell.com/NativeEdge

Sichern Sie Ihren wachsenden verteilten Betrieb, indem Sie die Sicherheit von Infrastruktur, Anwendungen, Daten, Netzwerken und NutzerInnen dauerhaft und automatisch verstärken, ohne dass ein Eingreifen der IT erforderlich ist.

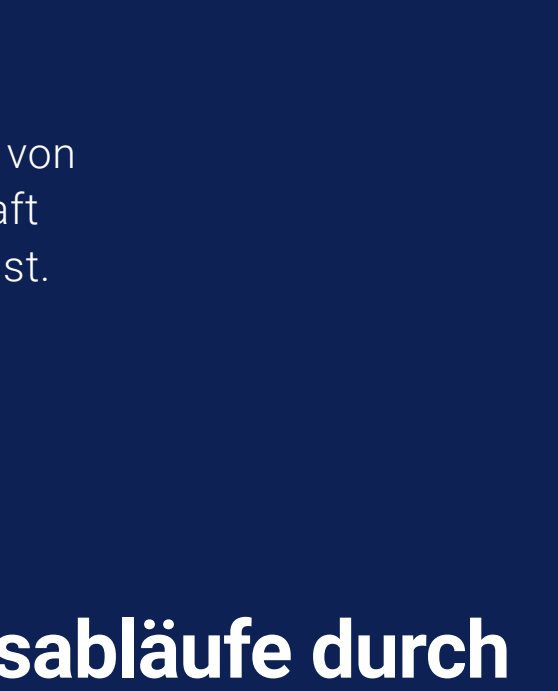
Dell NativeEdge schützt verteilte Betriebsabläufe durch

die Sicherstellung manipulationssicherer Hardware- und Softwareintegrität.



den Schutz von Daten und Anwendungen vom Edge über den Core bis zur Cloud.

die Durchsetzung von Zero-Trust-Prinzipien in der gesamten NativeEdge-Infrastruktur.



Stärkung der Zero-Trust-Sicherheit

Moderne Unternehmen sind für das Management von Tausenden von Anwendungen an geografisch verteilten Standorten verantwortlich und setzen oft auf eine heterogene Infrastruktur, die aus verschiedenen Komponenten besteht. Dadurch entsteht ein komplexes Netz von Technologiesilos, die ineffizient zu managen, schwierig zu sichern und langsam zu aktualisieren sind. Wenn Unternehmen weiterhin neue Anwendungen, neue Sensoren und neue Geräte an verteilten Standorten bereitstellen, wächst die Angriffsfläche für potenzielle Cyberbedrohungen.

Wie können Unternehmen die fortlaufende Sicherheit verteilter Datenvorgänge sicherstellen?

Mit Dell NativeEdge können Sie auf der Basis von Zero-Trust-Sicherheit zuverlässig arbeiten. Beim Einschalten eines Geräts wird eine hardwarebasierte Vertrauenskette hergestellt, die Funktionen wie UEFI Secure Boot und ein virtuelles Trusted Platform Module (vTPM) nutzt, um die Geräteintegrität sicherzustellen. NativeEdge unterstützt die DSGVO und andere globale Anforderungen an die Datenhoheit und bietet Sorgenfreiheit für verteilte Umgebungen. Dieser Ansatz schützt in Kombination mit Funktionen wie Zero-Trust-Mikrosegmentierung Ihre Anwendungen und Daten, sodass Sie überall sicher Innovationen entwickeln können.

Zero-Trust-Sicherheit

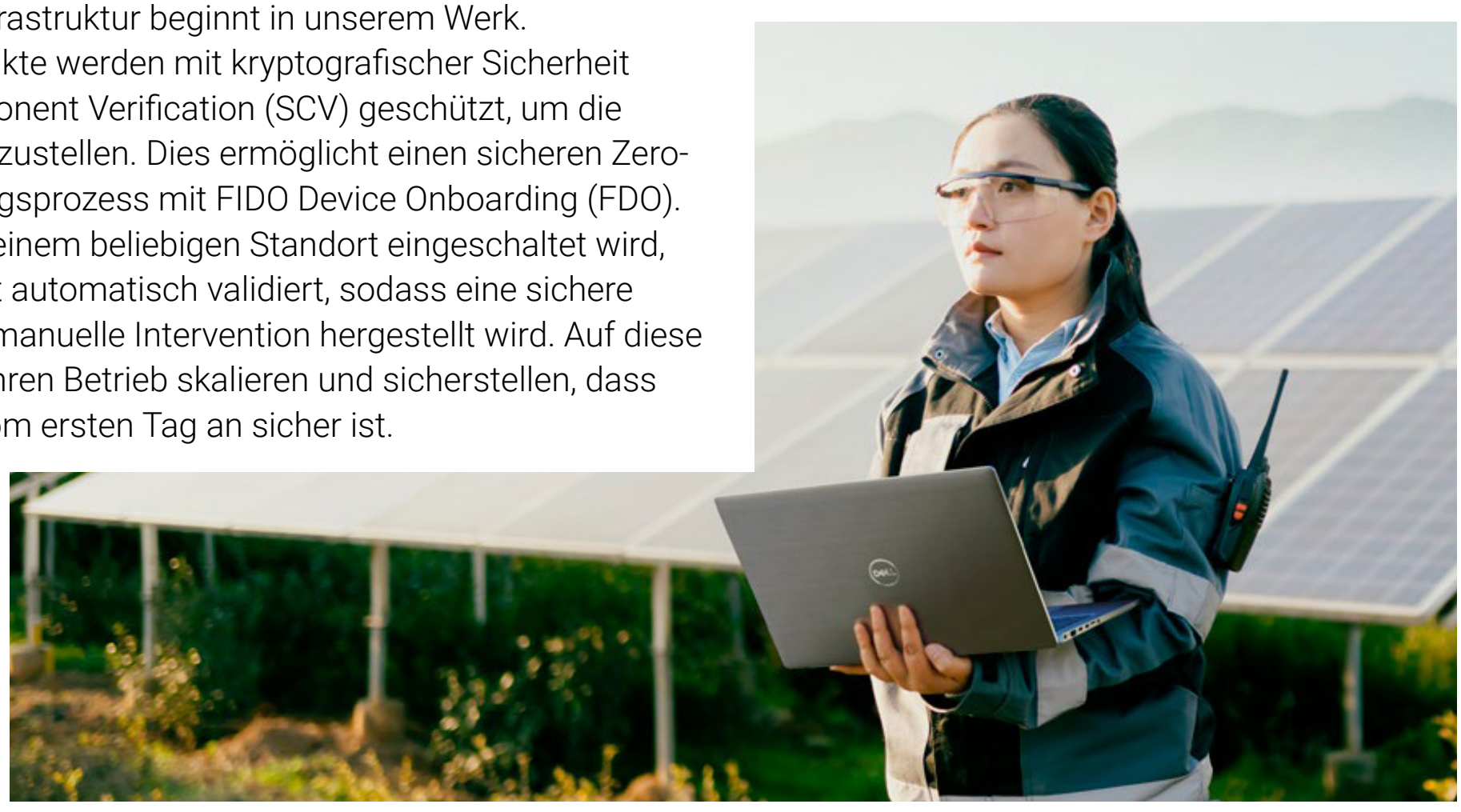
Der Sicherheitsstatus wird weiter gestärkt, weil alle Aktionen Ihrer Ressourcen überwacht werden und klar sind. Dies wird durch relevante Geschäftskontrollen, eine zentrale Steuerungsebene und eine Infrastruktur ermöglicht, die explizit in ihrem Namen arbeitet. Mit den Zero-Trust-Designprinzipien von NativeEdge können Unternehmen darauf vertrauen, dass die Integrität jeder verbundenen Ressource kontinuierlich bestätigt und validiert wird, wenn der verteilte Betrieb wächst.

Sicherstellung der Hardwareintegrität über die gesamte Lieferkette und ihren Lebenszyklus hinweg

Anhand der Beispiele eines Einzelhändlers oder Herstellers mit globalen Filialen oder Fabrikstandorten wird klar, wie schwierig es zunehmend wird, die vielfältige Hardware zu managen und zu sichern, die je nach Standort unterschiedliche Spezifikationen und Profile aufweist. Im Laufe der Zeit werden diese Geräte nicht kontinuierlich bestätigt und die Compliance kann nicht über einen längeren Zeitraum überprüft werden. Dieses Risiko wächst exponentiell, wenn mehrere Parteien an der Installation dieser Geräte beteiligt sind.

Wie können Sie eine verteilte Infrastruktur konsistent schützen?

Der Schutz Ihrer Infrastruktur beginnt in unserem Werk. NativeEdge-Endpunkte werden mit kryptografischer Sicherheit und Secured Component Verification (SCV) geschützt, um die Authentizität sicherzustellen. Dies ermöglicht einen sicheren Zero-Touch-Bereitstellungsprozess mit FIDO Device Onboarding (FDO). Wenn ein Gerät an einem beliebigen Standort eingeschaltet wird, wird seine Integrität automatisch validiert, sodass eine sichere Kontrollkette ohne manuelle Intervention hergestellt wird. Auf diese Weise können Sie Ihren Betrieb skalieren und sicherstellen, dass Ihre Infrastruktur vom ersten Tag an sicher ist.

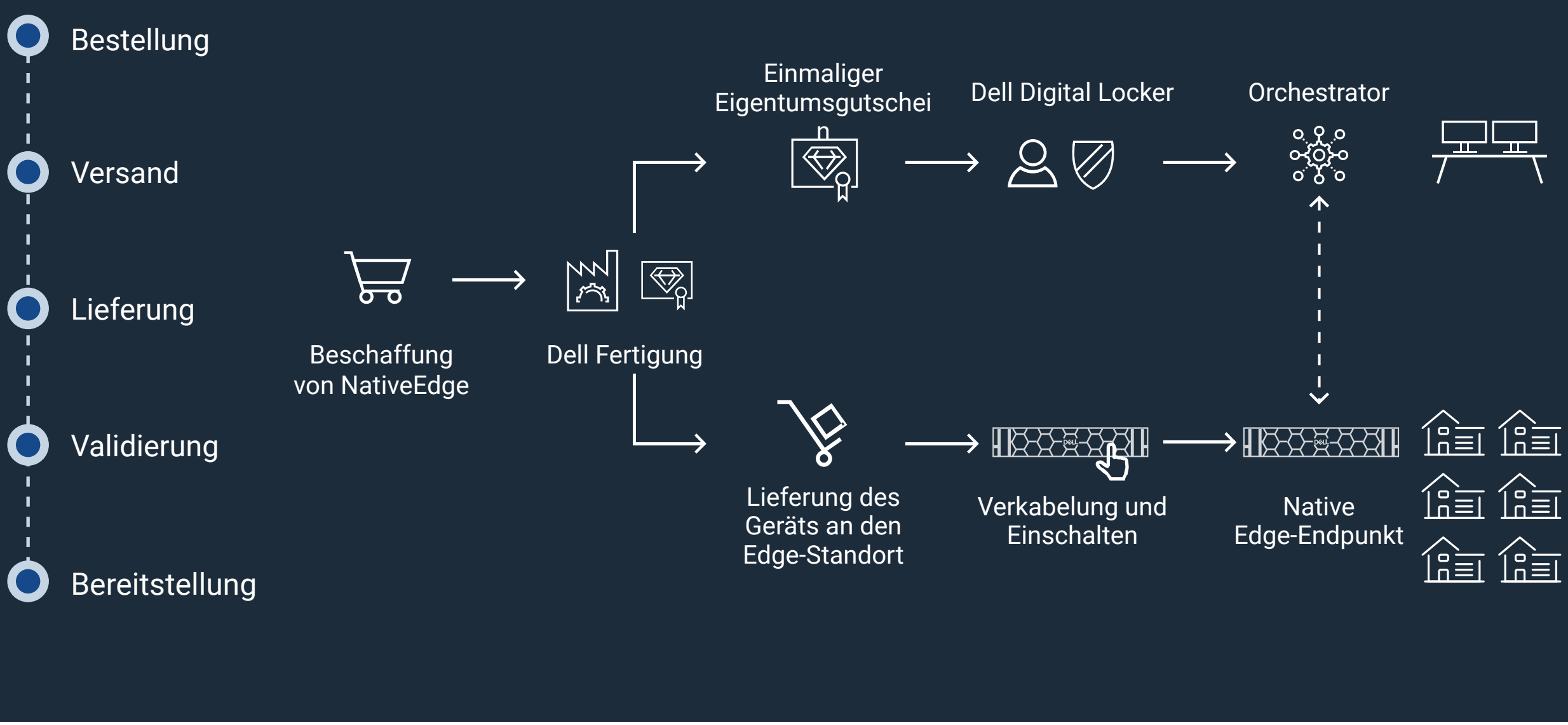


NativeEdge-Endpunkte sind für Kompatibilität mit NativeEdge optimiert und werden im Dell Werk mit kryptografischer Sicherheit geschützt.

NativeEdge nutzt den SCV-Prozess (Secured Component Verification), um die Authentizität und Integrität von Hardwarekomponenten sicherzustellen. Über SCV erzwingt NativeEdge die Integrität der Lieferkette, die Komponentenüberprüfung, die Firmwarevalidierung, sichere Startprozesse und kryptografische Signaturen, um den Schutz vor unbefugtem Zugriff oder Manipulationen zu gewährleisten.

Während diese Geräte den FIDO-basierten Geräteeinbindungsprozess durchlaufen, wird ihre Integrität automatisch zertifiziert, was die Sicherheit von der Fertigung im Dell Werk bis hin zu Empfang und Installation am Bereitstellungsstandort gewährleistet. Wenn Hardware in irgendeiner Weise manipuliert wird, isoliert die Plattform sie automatisch und schützt Vorgänge vor nicht autorisierten Elementen.

Sicheres Onboarding von Geräten und Zero-Trust-Framework

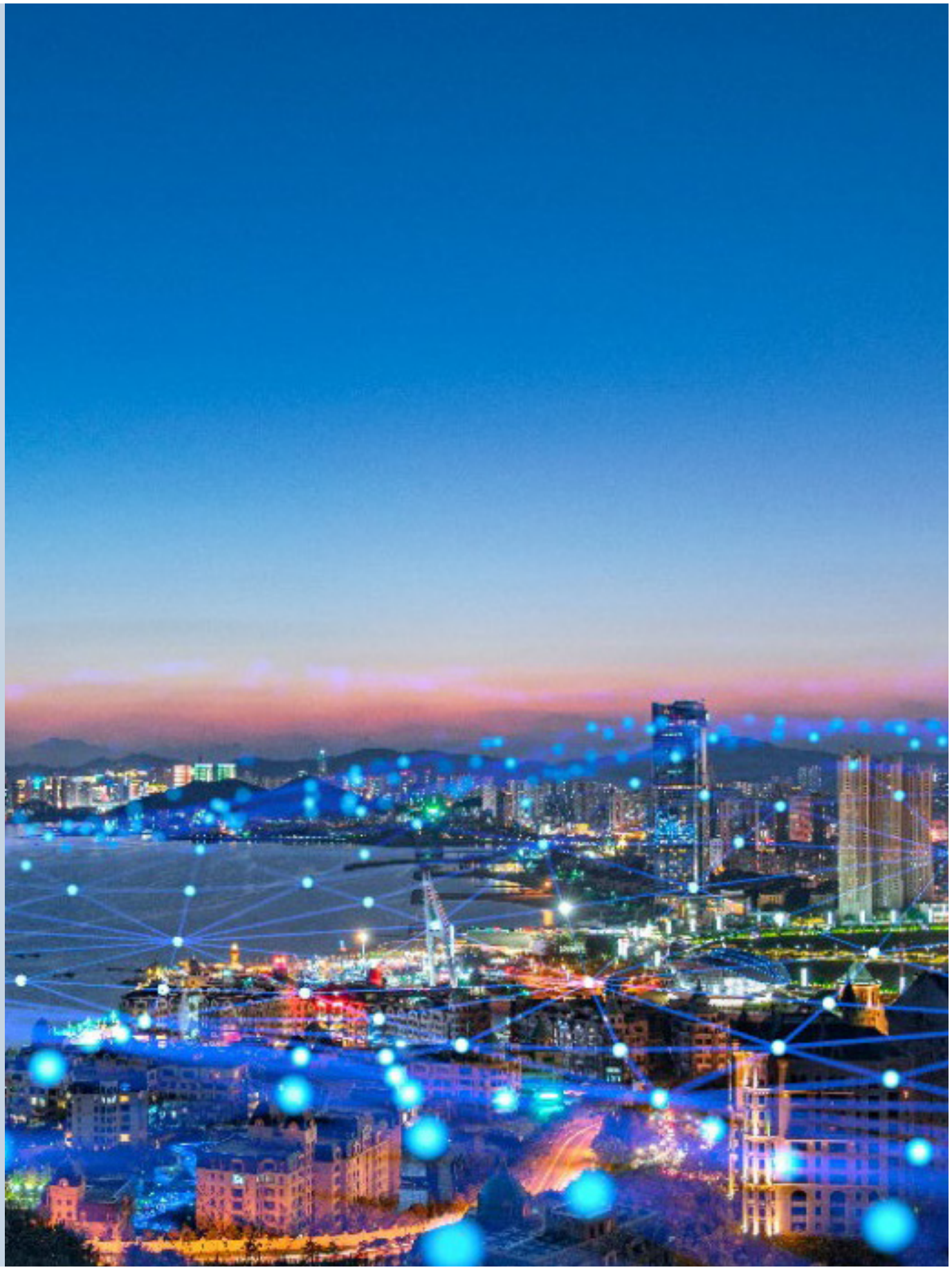


Geschützte Daten und Anwendungen vom Edge bis in die Cloud

Betrachten Sie das Beispiel eines globalen Einzelhändlers. Aufgrund der unterschiedlichen und verteilten Beschaffenheit von Einzelhandelsumgebungen werden die Identitäten von NutzerInnen, die auf Anwendungen und Workloads zugreifen, möglicherweise nicht routinemäßig überprüft. In diesen Fällen erfolgt der Zugriff lokal in dieser Umgebung und ist nicht zentral sichtbar und prüfbar.

Darüber hinaus haben Einzelhändler selten Einblick in die Softwarelieferkette bereitgestellter Anwendungen. Diese werden häufig von Managed Service Providers (MSPs) bearbeitet und es gibt möglicherweise keine transparenten automatisierten Prüfungen der Genauigkeit dieser Anwendungen. Diese Anwendungen werden häufig anfänglich von denselben MSPs konfiguriert, wobei die Möglichkeit besteht, dass die Konfiguration im Laufe der Zeit abweicht. Daher können StakeholderInnen nicht die Anwendungs-Compliance mit Sicherheits-Policies bestimmen.

Bei Fertigungsbetrieben führt das OT-Team (Operations Technology) in der Regel eine Vielzahl von Anwendungs-Workloads aus. Einige dieser Anwendungen kommunizieren mit Geräten wie PLCs und sind proprietäre Anwendungen, die keine interne Transparenz bieten.



Da IT- und OT-Netze logisch voneinander getrennt sind, werden die fortschrittlichen Sicherheitsfunktionen der IT nicht auf das OT-Netz übertragen. Deshalb verfügen Systeme und Anwendungen in den Produktionsnetzen von Fertigungsbetrieben nicht über die notwendigen Sicherheitskontrollen, um eine sichere OT-Umgebung zu gewährleisten. Ähnliche Herausforderungen im Zusammenhang mit der Anwendungs- und Datensicherheit sind in allen Branchen üblich.

Dell NativeEdge unterstützt Unternehmen dabei, die Datenpipeline von den Datenquellen zu den Anwendungen zu sichern, die lokal oder in der Cloud ausgeführt werden. Es kombiniert erweiterte Sicherheitsmaßnahmen wie Verschlüsselung, Nutzerzugriffskontrolle, Anwendungsblueprint-Katalog, Netzwerksegmentierung und Sicherheitsorchestrierung. Außerdem nutzt NativeEdge Telemetrie und Analysen, um den Sicherheitsstatus Ihrer verteilten Standorte proaktiv zu bewerten, ohne sich auf ExpertInnen mit Auditfunktionen verlassen zu müssen, die jeden Standort besuchen.

Erweiterte Sicherheitsfunktionen

Erweiterte Sicherheitsmaßnahmen sorgen für einen ausfallsicheren Betrieb

Zugriffskontrolle für NutzerInnen

NativeEdge bietet eine rollenbasierte Zugriffskontrolle (RBAC), um Zugriffsebenen basierend auf den Rollen und Zuständigkeiten von NutzerInnen zu analysieren. NutzerInnen der Geräte und bereitgestellten Anwendungs-Workloads werden in jeder Zugriffssitzung überprüft und durch Identitäts- und Zugriffsmanagement auf zentrale und transparente Weise bestätigt.

Netzwerksegmentierung

Die Mikrosegmentierung des Netzwerks für die Anwendungen erleichtert die Entwicklung und das Management von Richtlinien, die speziell auf diese Anwendungen abzielen, um sie noch sicherer zu machen. Dieser Ansatz mindert die Risiken potenzieller Sicherheitsverletzungen und die laterale Verschiebung von Bedrohungen in virtualisierten Umgebungen.

Katalog der Anwendungsblueprints

NativeEdge wurde entwickelt, um Anwendungen sicherer zu machen. Es beginnt mit einer sicheren Softwarelieferkette, die sich auf einen Katalog stützt, um Ihre Anwendungen mithilfe von Blueprints bereitzustellen. Der Katalog ist eine Sammlung von Blueprints zur Bereitstellung von Anwendungen von unabhängigen Softwareanbietern (ISVs) oder vorab validierten Blueprints von Dell, die von Unternehmen entwickelt wurden, um eine sichere Softwarelieferkette aufrechtzuerhalten. Diese Blueprints, die auf dem TOSCA-Standard und dem YAML-Format basieren, automatisieren die Bereitstellung von Anwendungen sowie KI-Frameworks auf vielen Edge-Geräten gleichzeitig. NativeEdge ermöglicht es Ihnen, proaktive Sicherheitskontrollen für bereitgestellte Anwendungen auf granularer Ebene festzulegen und stellt sicher, dass Ihre Anwendungen konsistent und in Übereinstimmung mit Ihren Sicherheitsrichtlinien bereitgestellt werden. Schließlich können die Anwendungs-Workloads auf NativeEdge-Endpunkten oder in einer Multi-Cloud-Umgebung als VMs und Container ausgeführt werden, die zentral von NativeEdge gemanagt werden.

Datenverschlüsselung und Data Protection

NativeEdge schützt Ihre Daten, wo auch immer sie sich befinden – im Ruhezustand, während der Übertragung und in Verwendung – vor Sicherheitsverletzungen und unbefugtem Zugriff. NativeEdge bietet eine robuste Data-at-Rest-Verschlüsselung (DARE), die die gesetzlichen Compliance-Standards erfüllt, um sicherzustellen, dass Ihre gespeicherten Daten verschlüsselt und vor physischem Diebstahl oder Manipulationen geschützt sind. NativeEdge verwaltet jede Datenressource mit Zero-Trust-Sicherheitsprinzipien, setzt eine strenge Zugriffskontrolle durch und überprüft diese kontinuierlich. Dies schützt nicht nur die Datenintegrität für Unternehmensanwendungen, sondern stärkt auch das Vertrauen aller geschäftlichen Stakeholder.

Sicherheitsorchestrierung

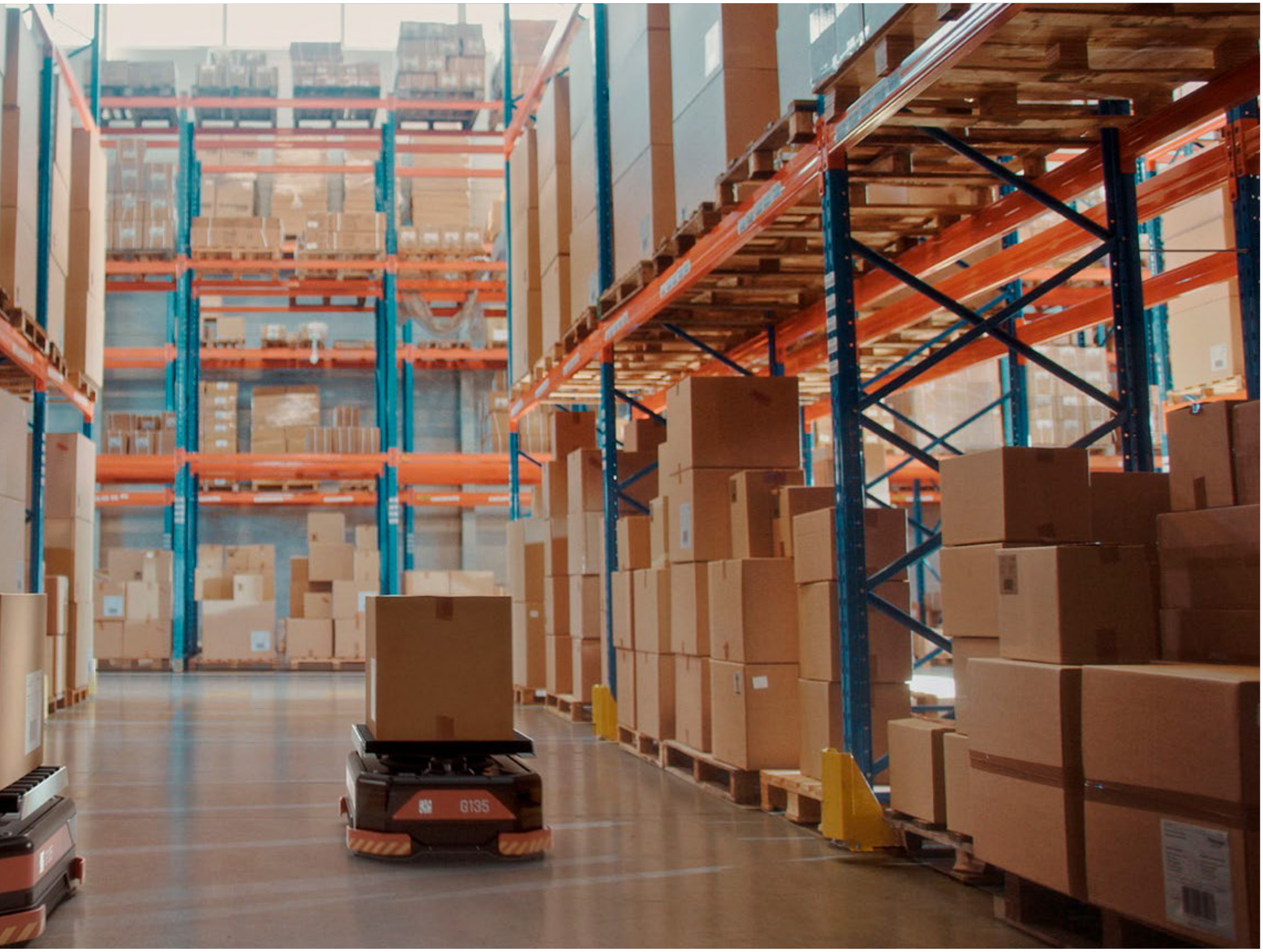
Unbefugte Aktionen/Ereignisse treten meist unbemerkt auf und werden oft nie behoben. Dies führt zu Risiken aufgrund manueller Prozesse und steht gegenüber hoch priorisierten Geschäftsaufgaben oft im Hintergrund. Darüber hinaus gibt es Unterschiede bei der IT-Integration rund um Identitätszugriffsmanagement (IAM)/rollenbasierte Zugriffskontrolle (RBAC) und Steuerungsebene.

Dies führt zu einer unkoordinierten Sicherheitsorchestrierung, die oft einzeln an jedem Standort verwaltet wird. In vielen OT-Infrastrukturen befinden sich diese Geräte in einer M2M-Umgebung (Machine-to-Machine) ohne Nutzererkennung. Eine zentralisierte Orchestrierung ist für diese Umgebungen von entscheidender Bedeutung.

NativeEdge sorgt für eine konsistente Sicherheitsorchestrierung im gesamten Edge-Bestand. Basierend auf der Gesamtzahl der Aktionen und Ereignisse, die in der Edge-Umgebung stattfinden, bietet es eine einheitliche Übersicht Ihres Sicherheitsstatus und ermöglicht eine zentralisierte Authentifizierung und eine konsistente Policy-Durchsetzung an allen Standorten. Es verwendet IAM- und RBAC-Funktionen, die ein sicheres Management der Plattform mit dem Prinzip der geringsten Berechtigungen ermöglichen und so den Detailgrad bieten, den Unternehmen benötigen. NativeEdge vereinfacht dank automatisiertem Protokollierungs- und Konfigurationsmanagement außerdem die Einhaltung von Bestimmungen wie DSGVO, PCI und HIPAA. So können Sie in jeder Umgebung zuverlässig arbeiten und Regeln wie Governance, Risiken und Compliance (GRC)/SecOps (Security Operations) integrieren.

Telemetrie und Analysen

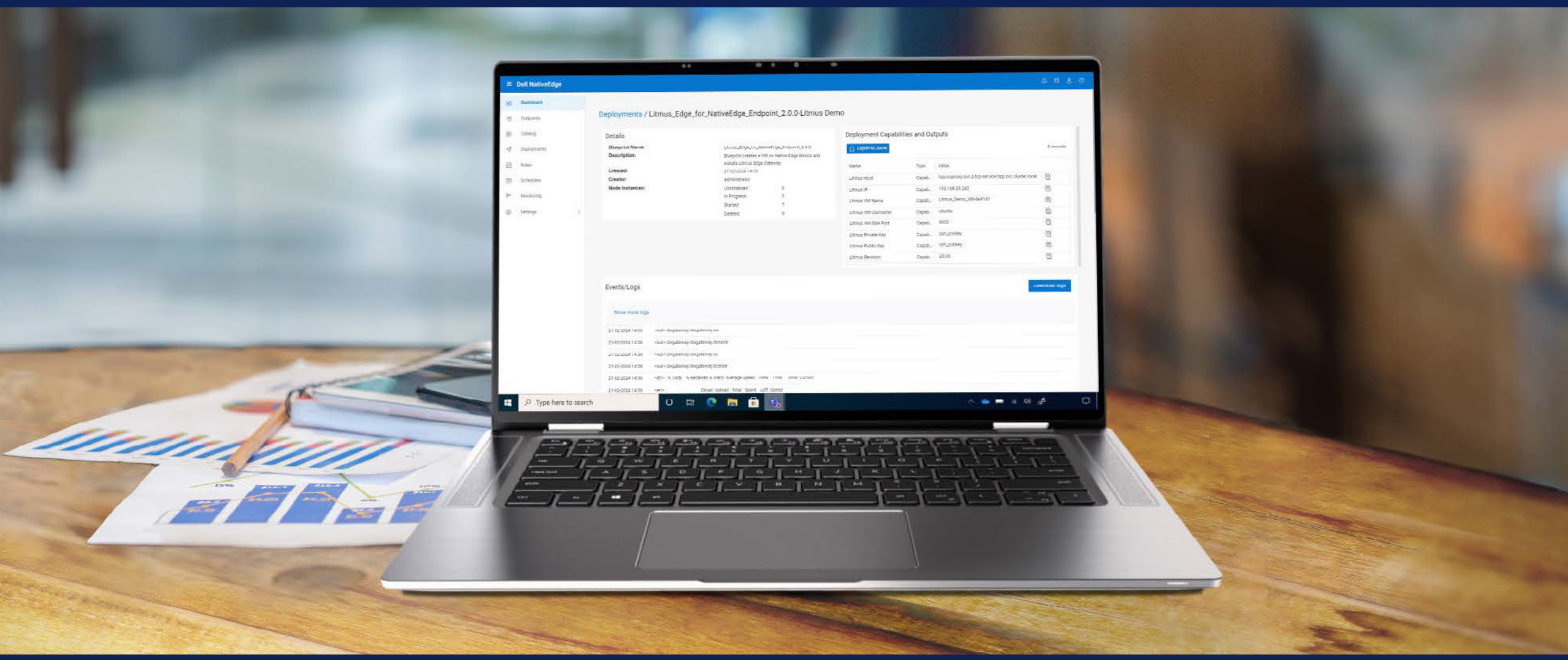
NativeEdge führt auf Basist von Telemetrie aus der Hardware- und Betriebsumgebung kontinuierlich Sicherheitsbewertungen gemäß definierten Compliancestandards durch. Diese werden verwendet, um die Erkennung von Konfigurationsabweichungen, Fehlkonfigurationen und die Notwendigkeit von Sicherheitsupdates zu bestimmen.



Schutz Ihrer Edge-Umgebung

Dell NativeEdge schützt Ihren Edge-Bestand mit Zero-Trust-Sicherheitsprinzipien, einschließlich FIDO-basiertem, sicherem Onboarding von Geräten in Kombination mit einem gehärteten und sicheren NativeEdge-Betriebssystem. Mit Dell NativeEdge können Sie sicher sein, dass Ihre Infrastruktur, Nutzer, Netzwerke, Anwendungen und Daten kontinuierlich über verteilte Standorte hinweg attestiert und validiert werden.

Schaffen Sie Innovationen, wo auch immer Sie arbeiten



DELL Technologies

Weitere Informationen unter **Dell.com/NativeEdge**

Veröffentlicht in den USA im Januar 2025.