Dell NativeEdge

Bescherming: werk vol vertrouwen met zero-trust-beveiliging

Tabel

Inhoud

Beveiliging in gedistribueerde omgevingen

Om in te spelen op de snel veranderende voorkeuren van klanten en marktdynamiek, implementeren organisaties nieuwe applicaties, updates en computinginfrastructuur in een ongeëvenaarde omvang en snelheid. Deze stortvloed aan data, infrastructuur en applicaties betekent dat het steeds belangrijker wordt om de gedistribueerde omgevingen waar deze nieuwe technologieën zich bevinden te beveiligen.

Naarmate bedrijven hun activiteiten uitbreiden, worden ze steeds kwetsbaarder voor veiligheidsrisico's, variërend van fysieke manipulatie van apparaten tot het hacken van data. Bovendien verwerken deze systemen vaak gevoelige persoonsgegevens, waardoor bedrijven een grotere verantwoordelijkheid hebben om hun klanten te beschermen.

Om activiteiten te beveiligen, moeten ondernemingen het volgende doen

Garantie
van de fysieke veiligheid van de infrastructuur die op gedistribueerde locaties wordt geïmplementeerd

Detectie
van apparaten die worden gemanipuleerd en bedreigingen aanpakken

Beheer
van de gebruikerstoegang op elk niveau

Schalen
van provisioning en software-updates op duizenden apparaten

Dell NativeEdge

Innoveer waar u ook werkt

Een volledige, end-to-end oplossing die de implementatie, indeling en levenscyclusbeheer van diverse infrastructuren en applicaties aan de edge en in gedistribueerde datacenters veilig centraliseert.

Vereenvoudig, optimaliseer en bescherm edge- en gedistribueerde datacenteromgevingen met functies zoals zero-touch onboarding, zero-trust beveiliging en geavanceerde workloadindeling. NativeEdge maakt gebruik van een KVM-hypervisor en containerruntime, waardoor organisaties zowel virtuele machines (VM's) als containers kunnen implementeren en beheren. Het is geoptimaliseerd om AI-workloads en -frameworks te coördineren, waardoor een naadloze implementatie en beheer van AI-gestuurde applicaties aan de edge en in gedistribueerde datacenters mogelijk is. NativeEdge kan zich ook aanpassen aan elke hardwareomgeving en ondersteunt een breed scala aan opties in verschillende vormfactoren, van Dell PowerEdge servers tot desktops en infrastructuur van derden.

Dell NativeEdge is speciaal gebouwd om de unieke uitdagingen van gedistribueerde omgevingen aan te pakken, zoals operationele complexiteit, schaalbaarheid en beveiliging. Het is een oplossing op maat voor moderne organisaties die zich richten op het benutten van de kracht van edge computing, terwijl ze tegelijkertijd kosten verlagen en efficiëntie verbeteren.

Eenvoudig
Bereik sneller resultaten en centraliseer activiteiten

Minder dan
1 minuut
om infrastructuur en applicaties te implementeren[1]

Optimize
Bereik naadloze virtualisatie en schaalbare AI

Tot
68%
tijdwinst door orkestratie van edge-applicaties te automatiseren[1]

Beschermen
Werk vol vertrouwen met zero-trust beveiliging

Maak 's werelds
veiligste
edge-activiteiten mogelijk[2]

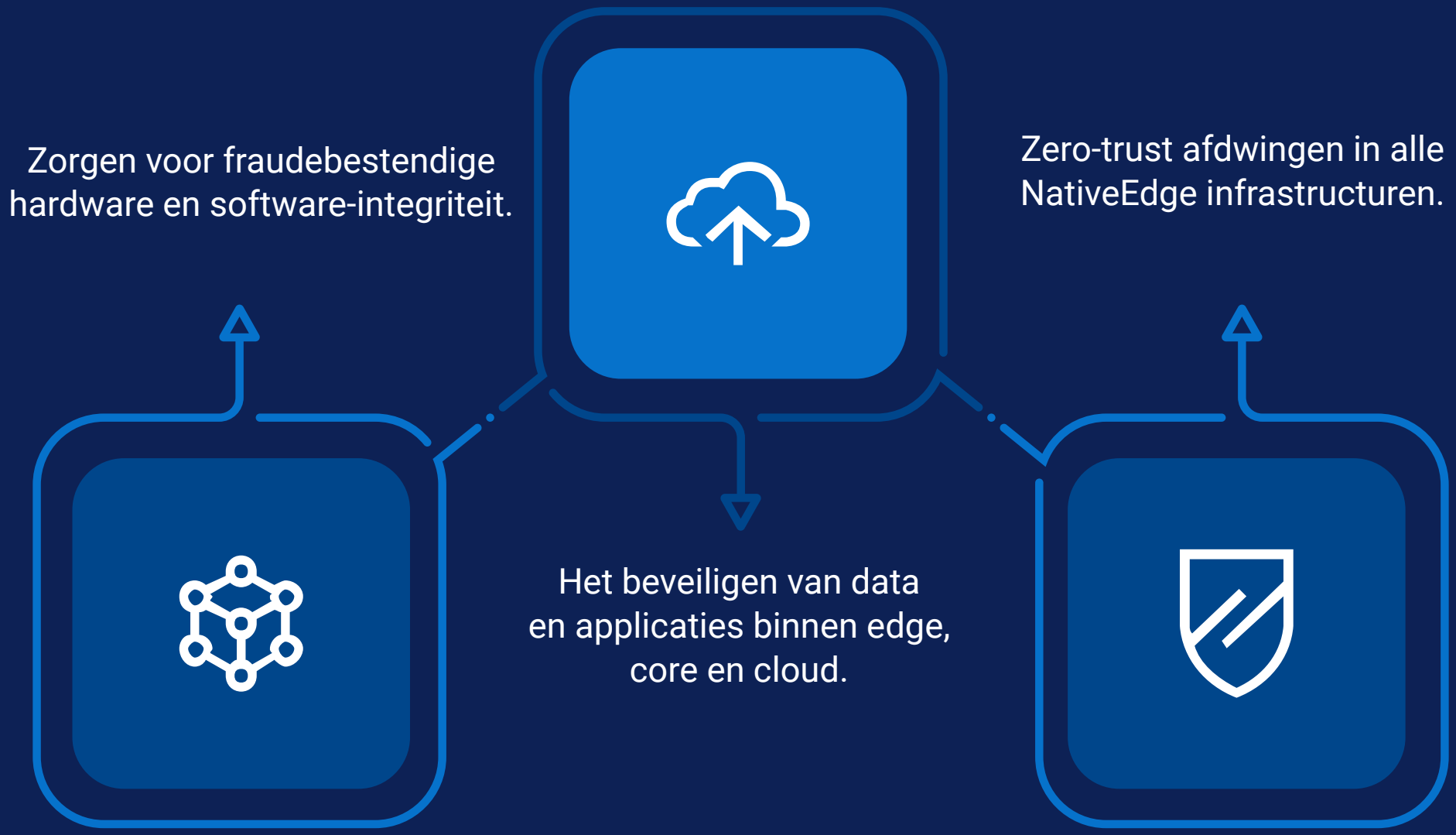
[1] Enterprise Strategy Group door TechTarget Technical Validation in opdracht van Dell Technologies, "Dell NativeEdge Edge Operations Software Platform", februari 2025.

[2] Gebaseerd op interne analyse door Dell Technologies, mei 2025.

Dell.com/NativeEdge

Beveilig uw groeiende gedistribueerde activiteiten door de beveiliging van infrastructuur, applicaties, gegevens, netwerk en gebruikers voortdurend en automatisch te versterken zonder enige tussenkomst van IT.

Dell NativeEdge beschermt gedistribueerde activiteiten als volgt:



Versterking van zero-trust beveiliging

Moderne ondernemingen zijn verantwoordelijk voor het beheer van duizenden applicaties verspreid over verschillende geografische locaties en zijn vaak afhankelijk van een heterogene mix van infrastructuur. Dit creëert een complex web van technologiesilo's die niet efficiënt te beheren, moeilijk te beveiligen en traag bij te werken zijn. Naarmate organisaties nieuwe applicaties, nieuwe sensoren en nieuwe apparaten blijven implementeren op gedistribueerde locaties, groeit het aanvalsoppervlak voor potentiële cyberdreigingen.

Hoe kunnen ondernemingen de voortdurende beveiliging van gedistribueerde data-activiteiten garanderen?

Dell NativeEdge stelt u in staat om met vertrouwen te werken op basis van zero-trust beveiliging. Vanaf het moment dat een apparaat wordt ingeschakeld, wordt een hardware-gebaseerde vertrouwensketen opgezet, waarbij gebruik wordt gemaakt van functies zoals UEFI Secure Boot en een virtuele Trusted Platform Module (vTPM) om de integriteit van het apparaat te waarborgen. NativeEdge biedt ingebouwde ondersteuning voor AVG en andere wereldwijde voorschriften voor datasoevereiniteit, wat gemoedsrust biedt voor gedistribueerde omgevingen. Deze aanpak, in combinatie met mogelijkheden zoals zero-trust microsegmentatie, beschermt uw applicaties en data, zodat u veilig kunt innoveren, waar u ook actief bent.

Zero-trust beveiliging

De beveiligingsmentaliteit wordt verder versterkt door alle acties van uw bronnen te monitoren en te begrijpen, mogelijk gemaakt door relevante bedrijfscontroles, een gecentraliseerd besturingsvlak en een infrastructuur die expliciet voor dit doel werkt. Met de Zero Trust-ontwerpprincipes van NativeEdge kunnen bedrijven erop vertrouwen dat naarmate gedistribueerde activiteiten toenemen, de integriteit van elke verbonden bron continu wordt geverifieerd en gevalideerd.

Zorgen voor hardware-integriteit in de hele leveringsketen en bijbehorende levenscyclus

Als we kijken naar de voorbeelden van een retailers of fabrikant met wereldwijde winkels of fabrieken, wordt het steeds moeilijker om de diverse hardware met verschillende specificaties en profielen op basis van locatie te beheren en te beveiligen. Na verloop van tijd worden deze apparaten niet continu gecertificeerd en kan de naleving niet op langere termijn worden gecontroleerd. Dit risico neemt exponentieel toe wanneer meerdere partijen betrokken zijn bij de installatie van deze apparaten.

Hoe kunt u gedistribueerde infrastructuur consistent beschermen?

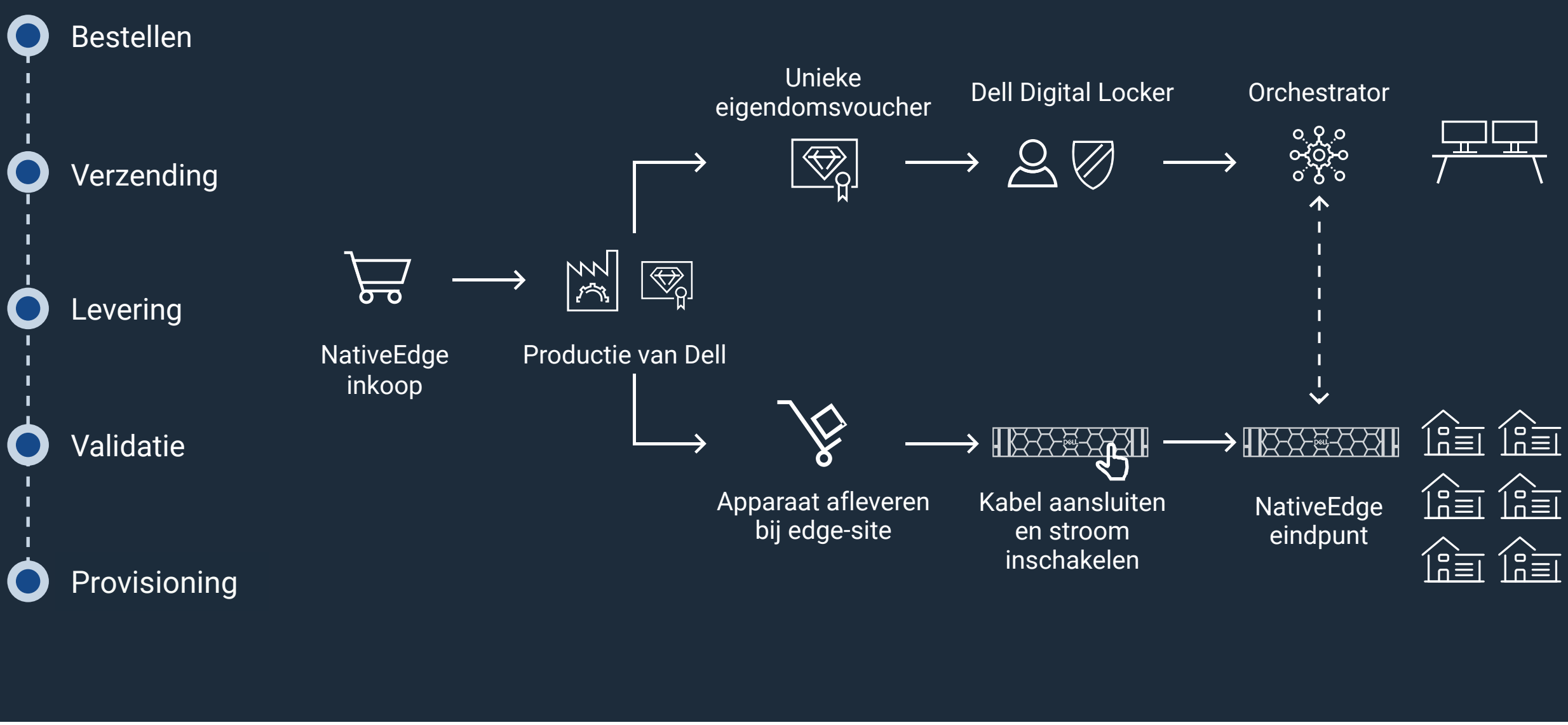
Het beschermen van uw infrastructuur begint in onze fabriek. NativeEdge-eindpunten worden beschermd met cryptografische beveiliging en Secured Component Verification (SCV) om authenticiteit te garanderen. Dit maakt een veilig, zero-touch implementatieproces mogelijk met behulp van FIDO Device Onboarding (FDO). Wanneer een apparaat op een willekeurige locatie wordt ingeschakeld, wordt de integriteit ervan automatisch gevalideerd, waardoor een veilige bewakingsketen ontstaat zonder handmatige tussenkomst. Hiermee kunt u uw activiteiten opschalen met de zekerheid dat uw infrastructuur vanaf dag één veilig is.

NativeEdge-eindpunten zijn geoptimaliseerd voor compatibiliteit met NativeEdge en worden beschermd met cryptografische beveiliging in de Dell fabriek.

NativeEdge maakt gebruik van het SCV-proces (Secured Component Verification) om de authenticiteit en integriteit van hardwarecomponenten te garanderen. Door middel van SCV zorgt NativeEdge voor de integriteit van de leveringsketen, componentverificatie, firmwarevalidatie, veilige opstartprocessen en cryptografische handtekeningen om ongeautoriseerde toegang of manipulatie te voorkomen.

Terwijl deze apparaten het op FIDO gebaseerde onboardingproces doorlopen, wordt hun integriteit automatisch gecertificeerd, waardoor de veiligheid wordt gewaarborgd vanaf de productie in de Dell fabriek tot aan de ontvangst en installatie op de implementatielocatie. Als er op enigerlei wijze met hardware wordt geknoeid, isoleert het platform deze automatisch, waardoor de werking wordt beschermd tegen kwaadwillende elementen.

Beveiligde onboarding van apparaten en een Zero Trust-framework

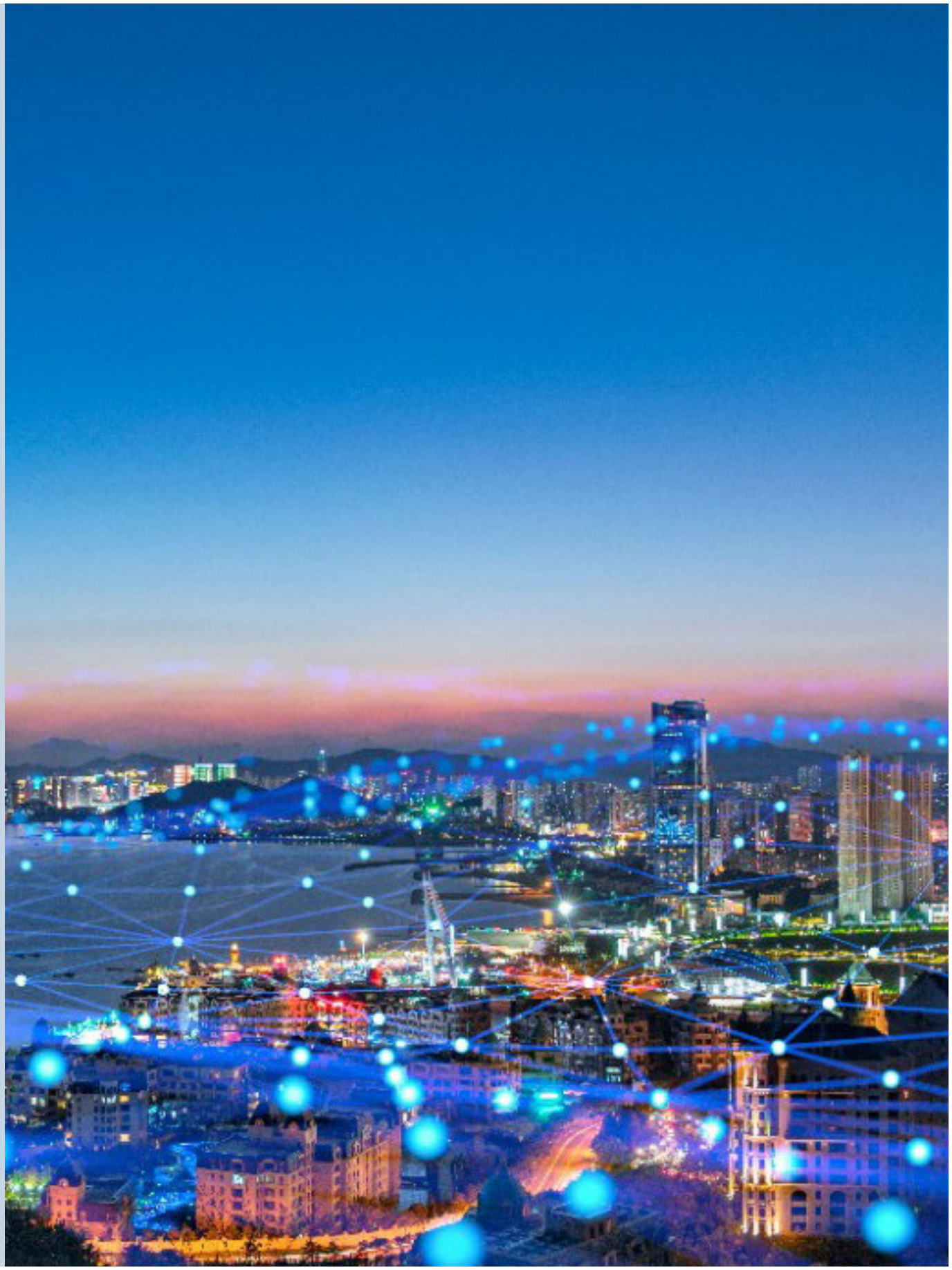


Versterkte data en applicaties van edge tot cloud

Denk aan het voorbeeld van een wereldwijde retailer. De uiteenlopende en gedistribueerde aard van retailomgevingen betekent dat de identiteit van gebruikers die toegang hebben tot applicaties en workloads mogelijk niet routinematig wordt geverifieerd. Als dat wel gebeurt, gebeurt dat lokaal in die omgeving en is het niet centraal zichtbaar en controleerbaar.

Bovendien hebben retailers zelden inzicht in de softwareleveringsketen van geïmplementeerde applicaties. Deze taken worden vaak uitgevoerd door Managed Service Providers (MSP's) en er zijn mogelijk geen zichtbare geautomatiseerde controles van de betrouwbaarheid van deze applicaties. Deze applicaties worden vaak in eerste instantie geconfigureerd door dezelfde MSP's, met de mogelijkheid dat de configuratie in de loop van de tijd afwijkt. Belanghebbenden kunnen daarom niet bepalen of applicaties voldoen aan het beveiligingsbeleid.

In het geval van fabrikanten voert het operationele technologie (OT)-team doorgaans een gevarieerde reeks applicatieworkloads uit. Sommige van deze applicaties werken samen met apparatuur zoals PLC's en zijn bedrijfseigen applicaties zonder interne zichtbaarheid.



IT-netwerkcapaciteiten worden niet doorgegeven aan het OT-netwerk, dat logisch gescheiden is. Het resultaat? Infrastructuur- en applicatieworkloads binnen de OT-netwerken van fabrikanten hebben geen toegang tot het niveau van netwerkbeveiligingsmaatregelen dat nodig is om een veilige OT-omgeving te faciliteren. Vergelijkbare uitdagingen op het gebied van applicatie- en databeveiliging zijn gangbaar in alle sectoren.

Dell NativeEdge helpt organisaties de datapipeline te beveiligen van databronnen naar de applicaties die lokaal of in de cloud worden uitgevoerd. Het combineert geavanceerde beveiligingsmaatregelen zoals encryptie, gebruikerstoegangscontrole, applicatieblauwdrukcatalogus, netwerksegmentatie en beveiligingscoördinatie. NativeEdge maakt ook gebruik van telemetrie en analyse om proactief de beveiligingsstatus van uw verspreide locaties te beoordelen, zonder dat experts met auditcapaciteiten elke locatie hoeven te bezoeken.

Geavanceerde beveiligingsmaatregelen

Geavanceerde beveiligingsmaatregelen zorgen voor veerkrachtige activiteiten

Toegangscontrole voor gebruikers

NativeEdge biedt op rollen gebaseerde toegangscontrole (RBAC) om toegangsniveaus te analyseren op basis van de rollen en verantwoordelijkheden van een gebruiker. Gebruikers van de apparaten en geïmplementeerde applicatieworkloads worden geverifieerd per toegangssessie en op een gecentraliseerde en zichtbare manier bevestigd via identiteits- en toegangsbeheer.

Netwerksegmentatie

Door het netwerk voor de applicaties te microsegmenteren, wordt het eenvoudiger om beleid te ontwikkelen en te beheren dat gericht is op deze applicaties om ze veiliger te maken. Deze aanpak vermindert de risico's van mogelijke inbreuken en de laterale verspreiding van bedreigingen binnen gevirtualiseerde omgevingen.

Catalogus met applicatieblauwdrukken

NativeEdge is ontworpen om applicaties veiliger te maken. Het begint met een veilige leveringsketen voor software die afhankelijk is van een catalogus om uw applicaties te implementeren met behulp van blauwdrukken. De catalogus is een verzameling blauwdrukken voor het implementeren van applicaties van onafhankelijke softwareleveranciers (ISV's) of vooraf gevalideerde blauwdrukken van Dell die door ondernemingen zijn ontwikkeld, allemaal om een veilige softwaretoeleveringsketen te behouden. Deze blauwdrukken, gebaseerd op de TOSCA-standaard en YAML-indeling, automatiseren de implementatie van applicaties en AI-frameworks op meerdere edge-apparaten tegelijk. Met NativeEdge kunt u proactieve beveiligingsmaatregelen instellen voor geïmplementeerde applicaties op een gedetailleerd niveau en ervoor zorgen dat uw applicaties consistent worden geïmplementeerd en in overeenstemming zijn met uw beveiligingsbeleid. Ten slotte kunnen de applicatieworkloads worden uitgevoerd op NativeEdge Endpoints of in een multicloudomgeving als VM's en containers, centraal beheerd door NativeEdge.

Dataversleuteling en -bescherming

NativeEdge beschermt uw gegevens waar ze zich ook bevinden – in rust, in transit en in gebruik – tegen inbreuken en ongeoorloofde toegang. NativeEdge biedt robuuste versleuteling van opgeslagen data (DARE), die voldoet aan federale nalevingsnormen, zodat uw opgeslagen data versleuteld en beschermd zijn tegen fysieke diefstal of manipulatie. NativeEdge beheert alle databronnen volgens zero-trust beveiligingsprincipes, waarbij strikte toegangscontrole wordt toegepast en de toegangscontrole voortdurend wordt gecontroleerd en geverifieerd. Dit beschermt niet alleen de data-integriteit voor bedrijfsapplicaties, maar verhoogt ook het vertrouwen van alle zakelijke belanghebbenden.

Beveiligingsindeling

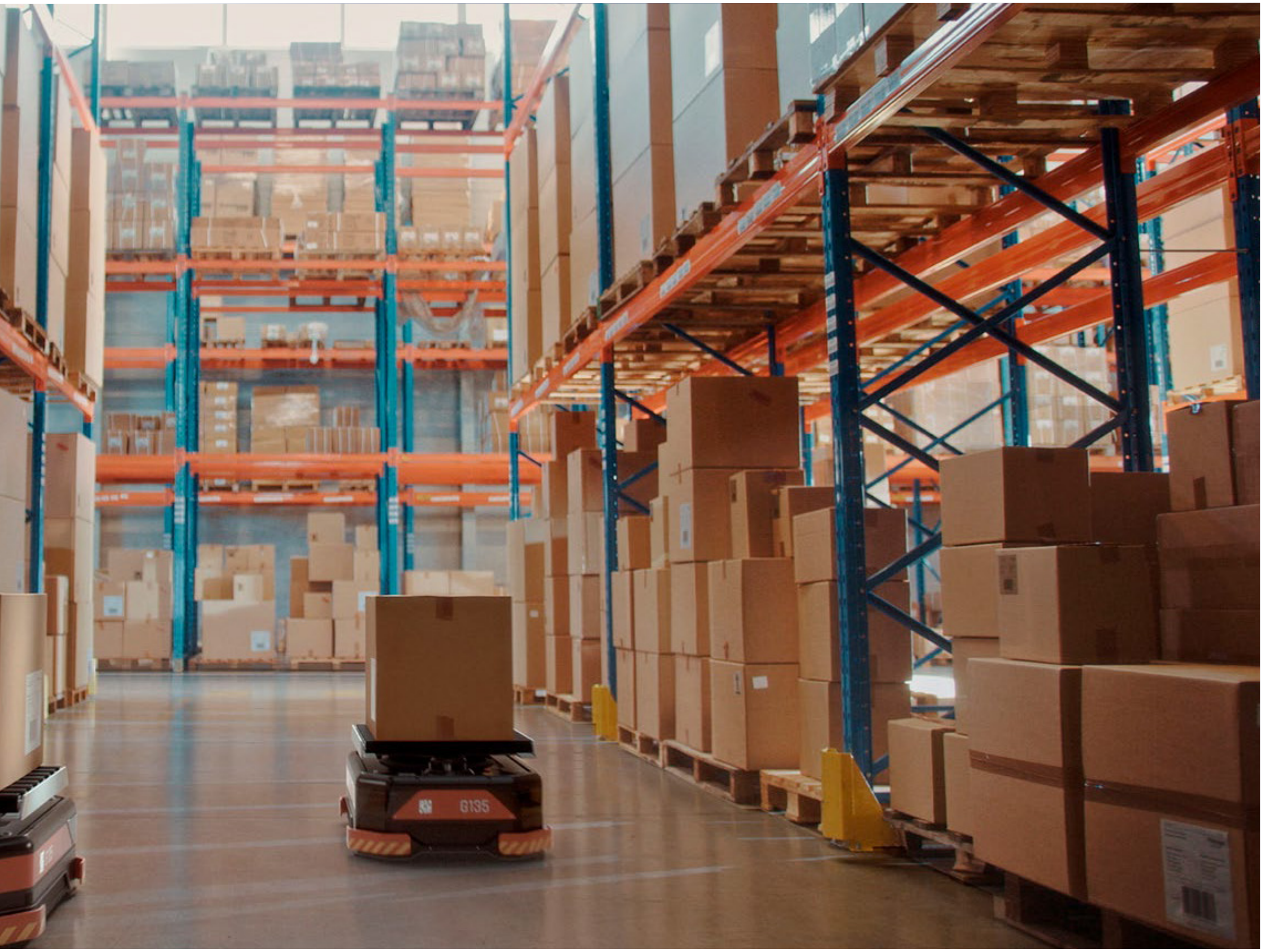
Ongeautoriseerde acties/gebeurtenissen vinden vaak onopgemerkt plaats en worden vaak nooit hersteld. Dit brengt risico's met zich mee vanwege handmatige processen en krijgt vaak minder prioriteit dan zakelijke taken met een hoge prioriteit. Bovendien bestaan er verschillen in IT-integratie rond Identity Access Management (IAM)/Role-Based Access Control (RBAC) en het besturingsvlak.

Dit leidt tot een onsamenhangende beveiligingsindeling die vaak op elke locatie afzonderlijk wordt beheerd. In veel OT-gevallen bevinden deze apparaten zich in een Machine-to-Machine (M2M)-omgeving waarin geen sprake is van gebruikersbewustzijn. Gecentraliseerde indeling is cruciaal voor deze omgevingen.

NativeEdge zorgt voor consistente beveiligingsindeling binnen de hele edge-omgeving. Op basis van het totaal aan acties en gebeurtenissen die plaatsvinden in de edge-omgeving, biedt het een uniform overzicht van uw beveiligingsstatus, waardoor gecentraliseerde authenticatie en consistente beleidsafdwinging op alle locaties mogelijk is. Het maakt gebruik van IAM- en RBAC-mogelijkheden die een veilig beheer van het platform mogelijk maken volgens het principe van minimale rechten, waardoor het de granulaire structuur biedt die ondernemingen nodig hebben. NativeEdge vereenvoudigt ook de naleving van regelgeving zoals de AVG, PCI en HIPAA door het loggen en configuratiebeheer te automatiseren, waardoor u met vertrouwen in elke omgeving kunt werken met de mogelijkheid om regels uit Governance, Risk en Compliance (GRC)/Security Operations (SecOps) te integreren.

Telemetrie en analytics

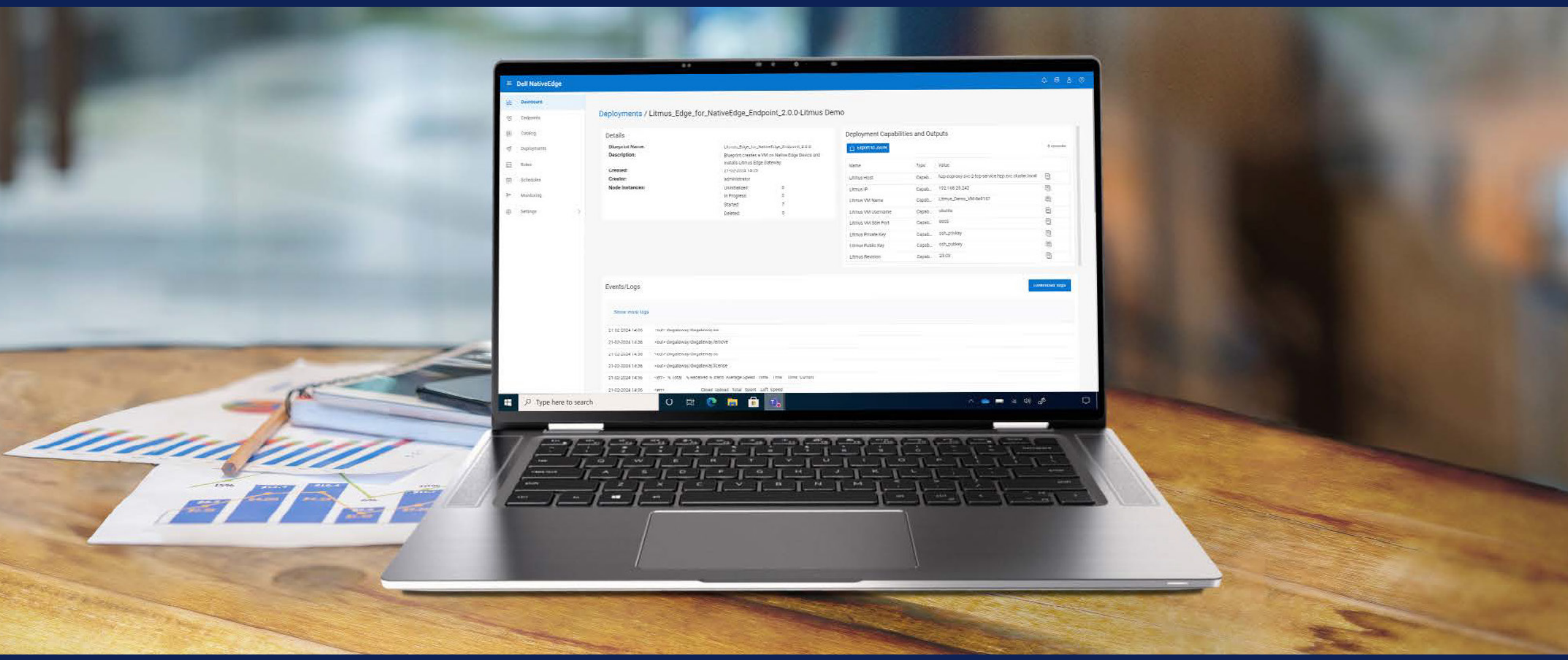
NativeEdge voert continu beveiligingsbeoordelingen uit in overeenstemming met gedefinieerde nalevingsnormen door gebruik te maken van telemetrie van de hardware en de bedrijfsomgeving. Deze worden gebruikt om configuratieafwijkingen, verkeerde configuraties en de noodzaak van beveiligingsupdates vast te stellen.



Bescherm uw edge-apparatuur

Dell NativeEdge beschermt uw edge-omgeving met zero-trust beveiligingsprincipes, waaronder op FIDO gebaseerde veilige onboarding van apparaten in combinatie met een versterkt en veilig NativeEdge besturingssysteem. Met Dell NativeEdge kunt u er zeker van zijn dat uw infrastructuur, gebruikers, netwerk, applicaties en data continu worden gevalideerd op gedistribueerde locaties.

Innoveer waar u ook werkt



DELL Technologies

Ga voor meer informatie naar **Dell.com/NativeEdge**