Dell NativeEdge

Skydda: Trygga verksamheten med nollförtroendesäkerhet

Tabell med

Innehålls-

Säkerhet i distribuerade miljöer

För att möta kundernas snabbt skiftande preferenser och marknadens dynamik distribuerar organisationer nya applikationer, uppdateringar och infrastruktur i en volym och hastighet som saknar motstycke. Denna störtflod av data, infrastruktur och applikationer innebär att det blir allt viktigare att säkra de distribuerade miljöer där dessa nya tekniker finns.

I takt med att företag expanderar sin kantmiljö, blir de alltmer sårbara för säkerhetsrisker – allt från manipulering av fysiska enheter till datahackning. Dessutom hanterar dessa system ofta känsliga personuppgifter, vilket lägger ett större ansvar på företagen att skydda sina kunder.

För att säkra verksamheten behöver företag

Säkerställa
den fysiska säkerheten för den infrastruktur som används på distribuerade platser

Upptäcka
manipulering av enheter och åtgärda hot

Kontrollera
användaråtkomst på samtliga nivåer

Skala
driftsättning och mjukvaruuppdateringar för tusentals enheter

Dell NativeEdge

Platsoberoende innovationsmöjligheter

En heltäckande fullstackslösning som på ett säkert sätt centraliserar distribution, orkestrering och livscykelhantering av olika infrastrukturer och applikationer både i kanten och i distribuerade datacenter.

Förenkla, optimera och skydda miljöer i kanten och distribuerade datacenter med funktioner som automatisk driftsättning, nollförtroendesäkerhet och avancerad samordning av arbetsbelastning. NativeEdge använder en KVM-hypervisor och en körtid för behållare som gör det möjligt för organisationer att distribuera och hantera både virtuella maskiner (VM) och behållare. Den är optimerad för att orkestrera AI-arbetsbelastningar och ramverk, vilket möjliggör sömlös distribution och hantering av AI-drivna applikationer i kanten och i distribuerade datacenter. NativeEdge kan också anpassas till alla hårdvarumiljöer och stöder ett brett utbud av alternativ i olika formfaktorer, från Dell PowerEdge-servrar till stationära datorer och infrastruktur från tredje part.

Dell NativeEdge är specialbyggt för att hantera de unika utmaningarna i distribuerade miljöer såsom operativ komplexitet, skalbarhet och säkerhet. Det är en lösning anpassad för moderna organisationer som fokuserar på att utnyttja kraften i kantdatabehandling samtidigt som kostnaderna minskar och effektiviteten förbättras.

Förenkla
Snabba upp resultaten och centralisera verksamheten

Det tar mindre än
1 minut
att distribuera infrastruktur och program[1]

Optimera
Uppnå sömlös virtualisering och skalbar AI

Upp till
68 %
tidsbesparingar genom automatisering av kantprogramorkestrering[1]

Skydda
Arbeta tryggt med nollförtroendesäkerhet

Möjliggör världens
säkraste
kantdrift[2]

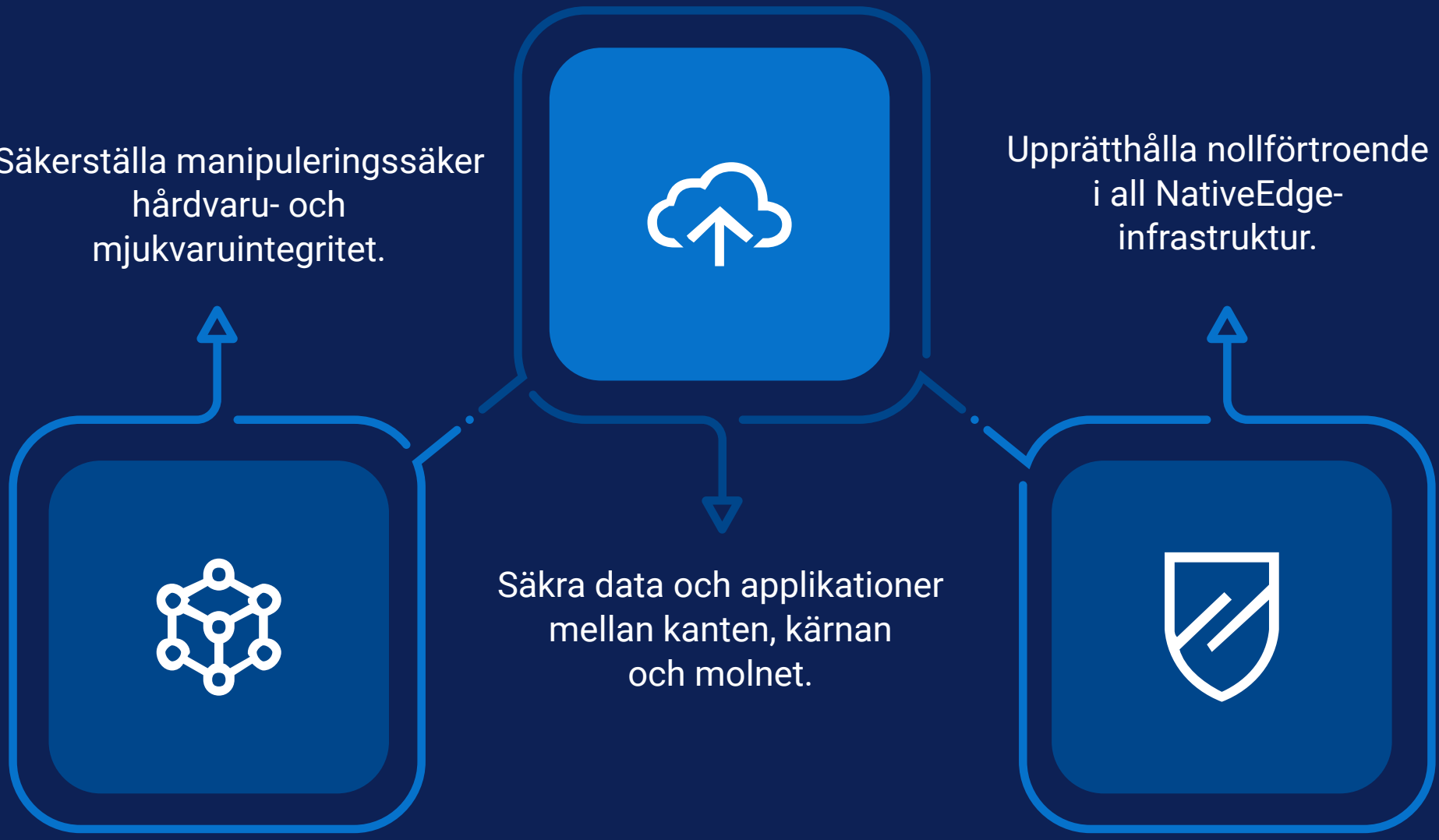
[1] Enterprise Strategy Group by TechTarget Technical Validation på uppdrag av Dell Technologies, "Dell NativeEdge - Edge Operations Software Platform", februari 2025.

[2]Enligt Dell Technologies interna analys, maj 2025.

Dell.com/NativeEdge

Säkra dina växande distribuerade verksamheter genom att ständigt och automatiskt stärka säkerheten för infrastruktur, applikationer, data, nätverk och användare helt utan IT-intervention.

Dell NativeEdge skyddar distribuerade verksamheter genom att



Skydda dig med nollförtroendesäkerhet

Moderna företag ansvarar för att hantera tusentals applikationer på geografiskt distribuerade platser och förlitar sig ofta på en heterogen blandning av infrastruktur. Detta skapar ett komplext nät av tekniska silostrukturer som är ineffektiva att hantera, svåra att säkra och tidskrävande att uppdatera. När organisationer fortsätter att distribuera nya applikationer, sensorer och enheter på distribuerade platser växer attackytan för potentiella cyberhot.

Hur kan företag säkerställa den fortlöpande säkerheten i distribuerad dataverksamhet?

Dell NativeEdge ger dig möjlighet att arbeta med tillförsikt tack vare en grund av nollförtroendesäkerhet. Från det ögonblick en enhet startas etableras en maskinvarubaserad förtroendekedja, vilken utnyttjar funktioner som UEFI Secure Boot och en virtuell Trusted Platform Module (vTPM) för att säkerställa enhetens integritet. NativeEdge har inbyggt stöd för GDPR och andra globala mandat för datasuveränitet, vilket ger trygghet i distribuerade miljöer. Detta tillvägagångssätt, i kombination med funktioner som nollförtroendebaserad mikrosegmentering, skyddar dina applikationer och data så att du kan vara innovativ på ett säkert sätt var du än befinner dig.

Säkerhet

Säkerhetsställningen stärks ytterligare genom övervakning och förståelse av alla resursernas handlingar, vilket möjliggörs av relevanta affärskontroller, ett centraliserat kontrollplan och en infrastruktur som uttryckligen arbetar för dess räkning. NativeEdge har designprinciper för nollförtroende som gör att företag kan lita på att i takt med att den distribuerade verksamheten växer, intygas och valideras integriteten hos varje ansluten resurs kontinuerligt.

Säkerställa hårdvarans integritet genom leveranskedjan och dess livscykel

Om man tittar på exemplen med en återförsäljare eller tillverkare med globala butiker eller fabriker blir det allt svårare att hantera och säkra den varierande hårdvara som har olika specifikationer och profiler baserat på plats. Med tiden intygas inte dessa enheter kontinuerligt, och efterlevnaden kan inte verifieras över en längre tidsperiod. Denna risk växer exponentiellt när flera parter är involverade i installationen av dessa enheter.

Hur kan du konsekvent skydda distribuerad infrastruktur?

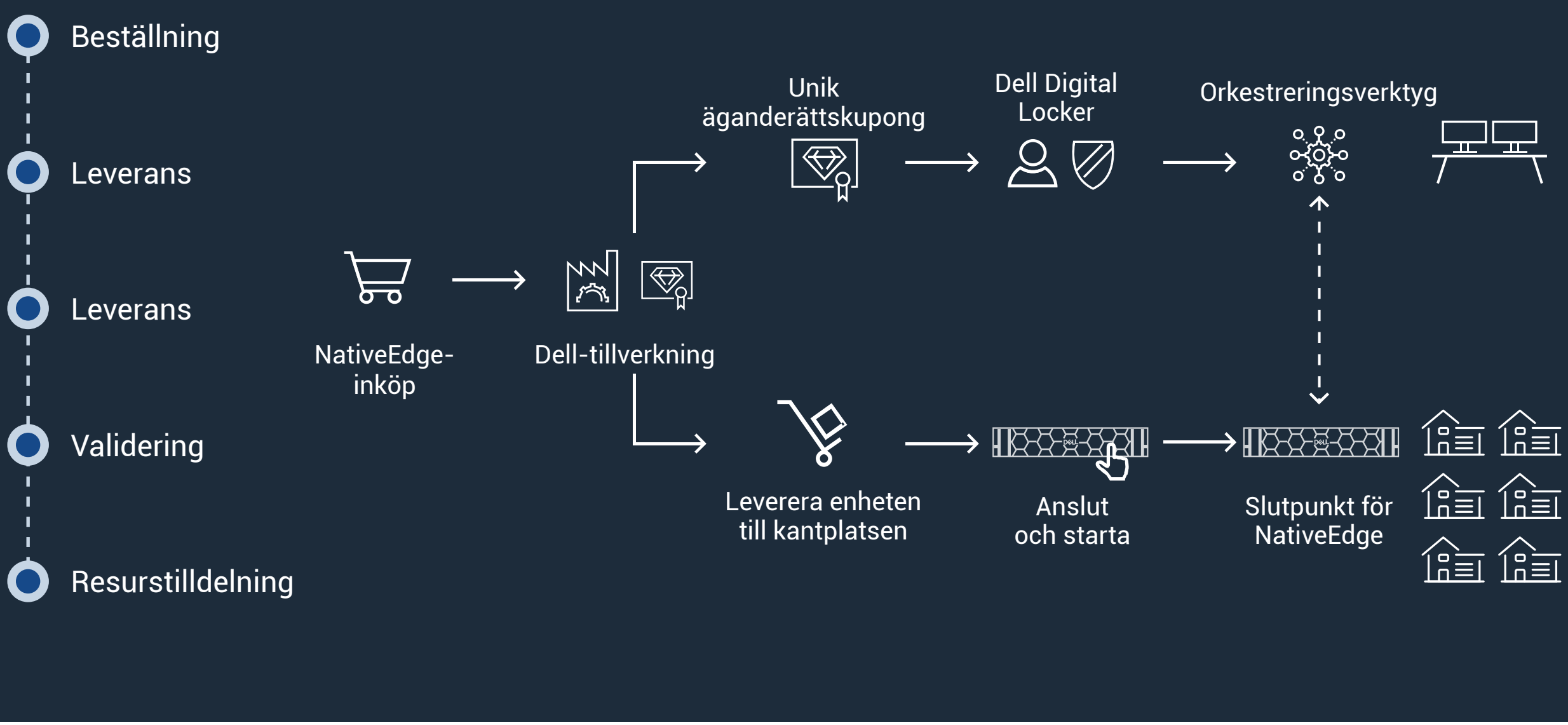
Skyddet av din infrastruktur börjar i vår fabrik. NativeEdge-slutpunkter skyddas med kryptografisk säkerhet och Secured Component Verification (SCV) för att säkerställa äktheten. Detta möjliggör en säker process för automatisk driftsättning med hjälp av FIDO Device Onboarding (FDO). När en enhet startas på valfri plats valideras dess integritet automatiskt, vilket etablerar en säker ansvarskedja utan manuell intervention. Detta gör att du kan skala din verksamhet med vetskap om att din infrastruktur är säker från dag ett.

NativeEdge-slutpunkter är optimerade för kompatibilitet med NativeEdge och skyddas med kryptografisk säkerhet i Dells fabrik.

NativeEdge utnyttjar processen Secured Component Verification (SCV) för att säkerställa äktheten och integriteten hos hårdvarukomponenter. Genom SCV upprätthåller NativeEdge leveranskedjans integritet, komponentverifiering, validering av inbyggd mjukvara, säkra startprocesser och kryptografiska signaturer för att skydda mot obehörig åtkomst eller manipulering.

När dessa enheter genomgår den FIDO-baserade processen för driftsättning certifieras deras integritet automatiskt, vilket säkerställer säkerheten hela vägen från tillverkningen i Dells fabrik till mottagande och installation på platsen. Om hårdvaran manipuleras på något sätt isolerar plattformen dem automatiskt, vilket skyddar verksamheten från skadliga element.

Säker enhetsintroduktion och ett nollförtroenderamverk

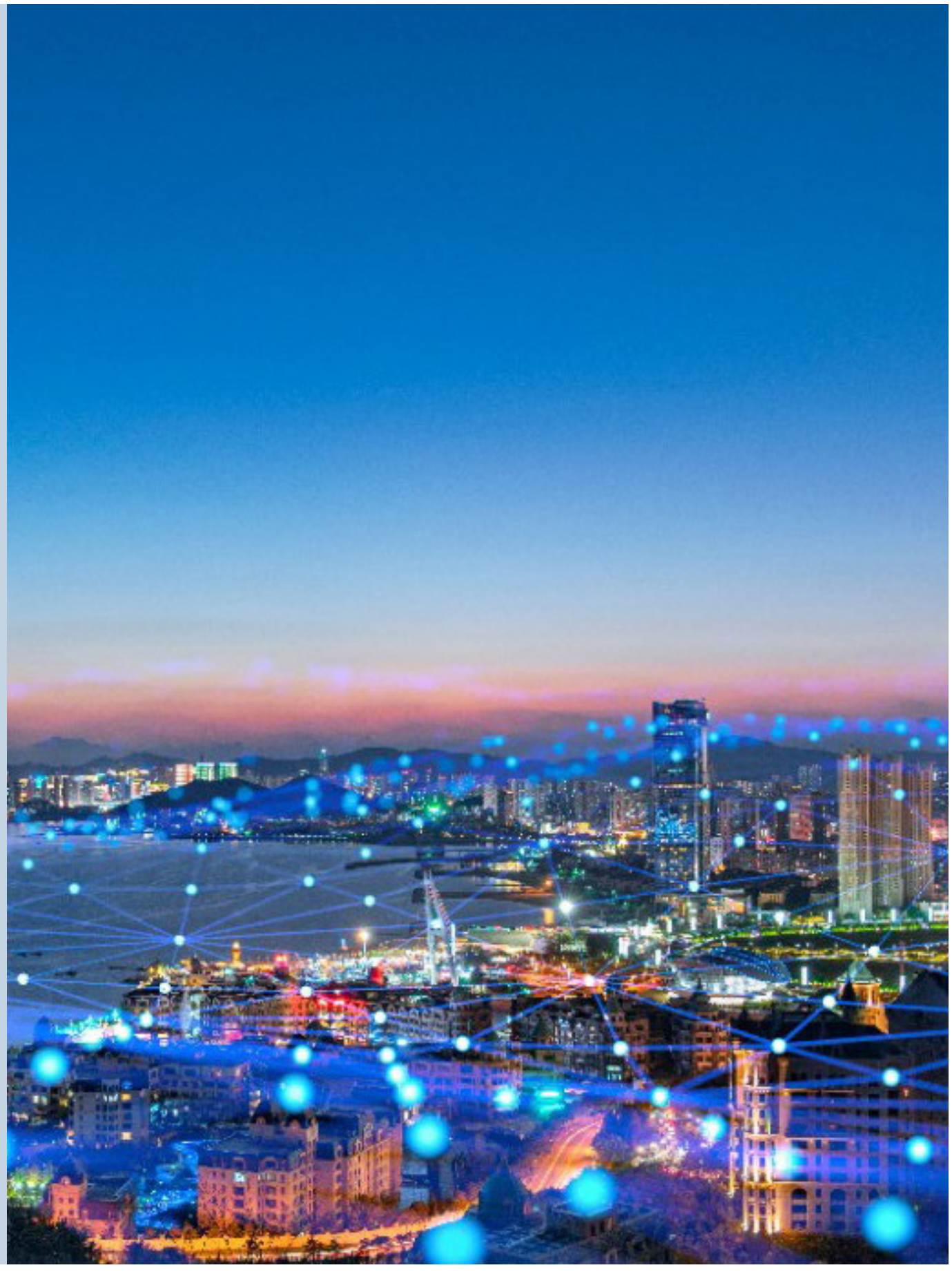


Förstärkt skydd för data och applikationer, från kanten till molnet

Tänk dig exemplet med en global återförsäljare. Butiksmiljöernas spridda och distribuerade natur innebär att identiteterna för användare som får åtkomst till applikationer och arbetsbelastningar kanske inte verifieras rutinmässigt. Om de gör det är det lokalt i den miljön och inte centralt synligt eller granskningsbart.

Dessutom har återförsäljare sällan insyn i leveranskedjan för mjukvaran i de distribuerade applikationerna. Dessa hanteras ofta av Managed Service Providers (MSP) och det finns kanske inga synliga automatiska kontroller av dessa appars tillförlitlighet. Dessa applikationer konfigureras ofta initialt av samma MSP:er, med risken att konfigurationen driver iväg över tid. Därför kan intressenter inte fastställa om applikationen följer säkerhetspolicyerna.

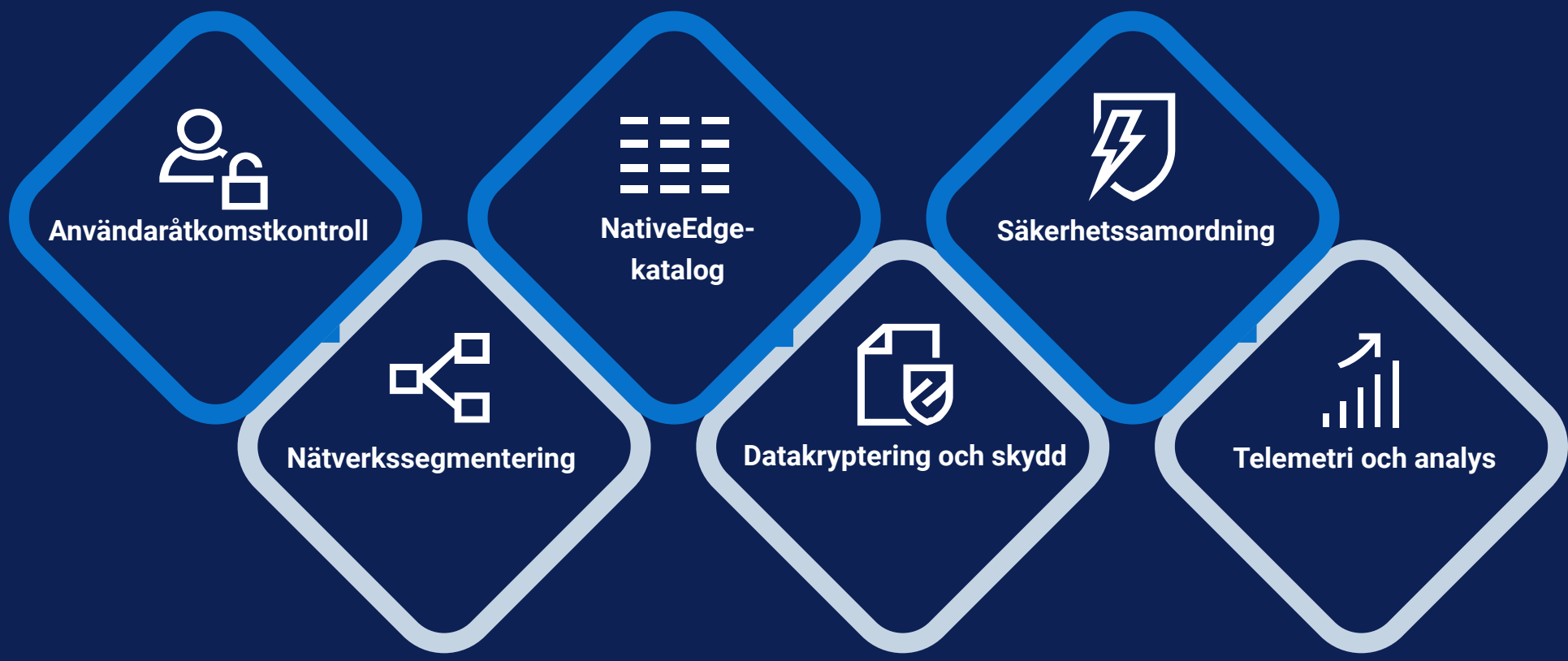
När det gäller tillverkare kör teamet för operativ teknik (OT) vanligtvis en varierad uppsättning applikationsarbetsbelastningar. Vissa av dessa applikationer kommunicerar med utrustning som PLC:er och är proprietära applikationer utan intern insyn.



IT-nätverkskapacitet når inte ner till OT-nätverket, vilket är logiskt separat. Vilket resulterar i infrastruktur och applikationsarbetsbelastningar inom tillverkarnas OT-nätverk som inte har tillgång till den nivå av nätverkssäkerhetskontroller som krävs för att underlätta en säker OT-miljö. Liknande utmaningar relaterade till applikations- och datasäkerhet är vanliga inom alla branscher.

Dell NativeEdge hjälper organisationer att säkra datapipelinen från datakällor till applikationerna som körs lokalt eller i molnet. Den kombinerar avancerade säkerhetsåtgärder såsom kryptering, användaråtkomstkontroll, katalog för applikationsmallar, nätverkssegmentering och säkerhetssamordning. NativeEdge använder även telemetri och analys för att proaktivt bedöma säkerhetsställningen på dina distribuerade platser utan att behöva förlita sig på att experter med granskningskapacitet besöker varje plats.

Avancerade säkerhetsåtgärder



Avancerade säkerhetsåtgärder säkerställer verksamhetens motståndskraft

Användaråtkomstkontroll

NativeEdge erbjuder rollbaserad åtkomstkontroll (RBAC) för att analysera åtkomstnivåer baserat på användarens roller och ansvarsområden. Användare av enheterna och distribuerade applikationsarbetsbelastningar verifieras per åtkomstsession samt intygas på ett centraliserat och synligt sätt genom identitets- och åtkomsthantering.

Nätverkssegmentering

Mikrosegmentering av nätverket för applikationerna gör det enklare att utveckla och hantera policyer som riktar sig mot dessa applikationer för att göra dem säkrare. Detta tillvägagångssätt minskar riskerna för potentiella intrång och förflyttning av hot i sidled inom virtualiserade miljöer.

Katalog för applikationsmallar

NativeEdge är utformat för att göra applikationer säkrare. Detta börjar med en säker leveranskedja för mjukvara som förlitar sig på en katalog för att distribuera dina applikationer med hjälp av mallar. Katalogen är en samling mallar för att distribuera applikationer från oberoende mjukvaruleverantörer (ISV:er) eller förauktoriserade mallar från Dell utvecklade av företag, allt för att upprätthålla en säker leveranskedja för mjukvara. Dessa mallar, baserade på TOSCA-standard och YAML-format, automatiserar driftsättningen av applikationer såväl som AI-ramverk över många kantenheter samtidigt. NativeEdge ger möjlighet att ställa in proaktiva säkerhetskontroller för distribuerade applikationer på en detaljerad nivå och säkerställer att dina applikationer distribueras konsekvent och i linje med dina säkerhetspolicyer. Slutligen kan applikationsarbetsbelastningarna köras på slutpunkter för NativeEdge eller i en flermolnsmiljö som virtuella maskiner och containrar, vilket hanteras centralt av NativeEdge.

Datakryptering och skydd

NativeEdge skyddar dina data var de än finns, lagrade, under överföring och under användning, mot intrång och obehörig åtkomst. NativeEdge erbjuder robust kryptering av data vid vila (DARE), som uppfyller nationella efterlevnadsstandarder, vilket säkerställer att dina lagrade data är krypterade och skyddade mot fysisk stöld eller manipulering. NativeEdge styr varje dataresurs med nollförtroendeprinciper, vilket upprätthåller strikt åtkomstkontroll och kontinuerligt intygar och verifierar åtkomstkontrollen. Detta skyddar inte bara dataintegriteten för företagsapplikationer utan ökar även förtroendet hos alla affärsintressenter.

Säkerhetssamordning

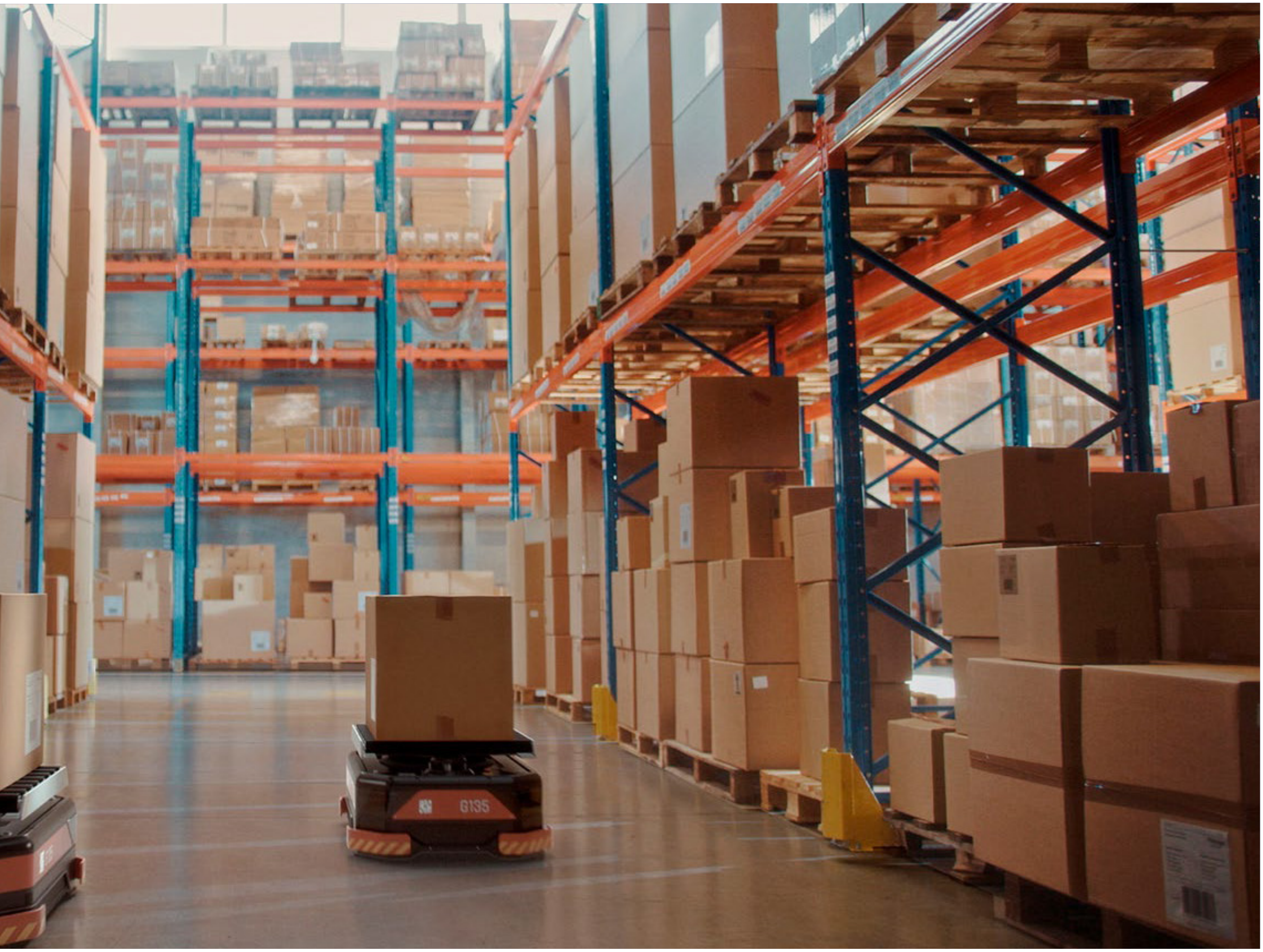
Obehöriga handlingar eller händelser sker ofta obemärkt och åtgärdas ofta aldrig. Detta medför risker på grund av manuella processer och prioriteras ofta ner till förmån för högt prioriterade affärsuppgifter. Dessutom finns det variationer inom IT-integrering gällande identitets- och åtkomsthantering (IAM), rollbaserad åtkomstkontroll (RBAC) och kontrollplan.

Detta leder till en fragmenterad säkerhetssamordning vilken ofta hanteras individuellt på varje plats. I många OT-fall finns dessa enheter i en maskin-till-maskin-miljö (M2M) som saknar användarkännedom. Centraliserad samordning är avgörande för dessa miljöer.

NativeEdge säkerställer konsekvent säkerhetssamordning i hela kanten. Baserat på det samlade resultatet av handlingar och händelser som sker i kantmiljön ger den en enhetlig vy över din säkerhetsställning, vilket möjliggör centraliserad autentisering och konsekvent policyupprätthållande på alla platser. Den använder IAM- och RBAC-funktioner som tillåter säker hantering av plattformen enligt principen om minsta möjliga privilegium, vilket ger den detaljrikedom som företag behöver. NativeEdge förenklar även efterlevnad av regler som GDPR, PCI och HIPAA genom att automatisera loggning och konfigurationshantering, vilket hjälper dig att arbeta med tillförsikt i alla miljöer med möjligheten att inkludera regler från styrning, risk och efterlevnad (GRC) samt säkerhetsverksamhet (SecOps).

Telemetri och analys

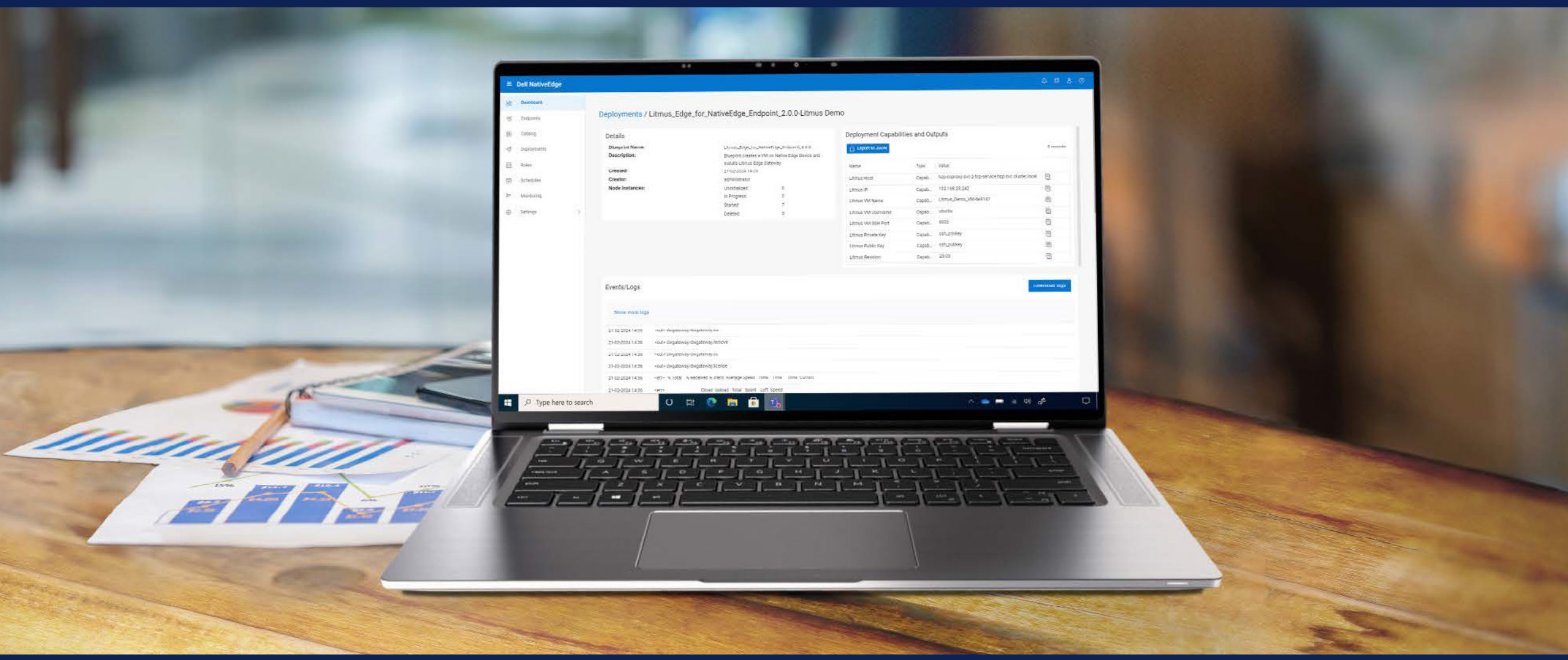
NativeEdge utför kontinuerligt säkerhetsbedömningar i linje med definierade efterlevnadsstandarder genom att förlita sig på telemetri från hårdvaran och driftsmiljön. Dessa används för att upptäcka konfigurationsdrift, felkonfigurationer och behovet av säkerhetsuppdateringar.



Skydda din kantegendom

Dell NativeEdge skyddar din kantegendom med nollförtroendeprinciper inklusive FIDO-baserad säker driftsättning av enheter kopplat till ett härdat och säkert NativeEdge OS. Med Dell NativeEdge kan du lita på att din infrastruktur, dina användare, ditt nätverk, dina applikationer och dina data kontinuerligt intygas och valideras på distribuerade platser.

Platsoberoende innovationsmöjligheter



DELL Technologies

Mer information om **Dell.com/NativeEdge**