Dell NativeEdge

Ochrona: działaj pewnie dzięki zabezpieczeniom opartym na modelu „zero trust”

Spis

Spis treści

Bezpieczeństwo w środowiskach rozproszonych

Aby sprostać szybko zmieniającym się preferencjom klientów i dynamice rynku, organizacje wdrażają nowe aplikacje, aktualizacje i infrastrukturę obliczeniową w niespotykanej dotąd skali i tempie. Ten zalew danych, infrastruktury i aplikacji oznacza, że coraz ważniejsze staje się zabezpieczenie środowisk rozproszonych, w których znajdują się te nowe technologie.

W miarę rozszerzania operacji przedsiębiorstwa stają się coraz bardziej narażone na ataki, takie jak fizyczna ingerencja w urządzenia czy hakowanie danych. Ponadto systemy te często przetwarzają wrażliwe dane osobowe, co nakłada na przedsiębiorstwa większą odpowiedzialność za ochronę swoich klientów.

Aby zapewnić bezpieczeństwo operacji, przedsiębiorstwa muszą

Zagwarantować
bezpieczeństwo fizyczne infrastruktury rozmieszczonej w różnych lokalizacjach

Wykrywać
manipulacje przy urządzeniach i eliminować zagrożenia

Kontrolować
dostęp użytkowników na każdym poziomie

Skalować
zasoby i aktualizacje oprogramowania na tysiącach urządzeń

Dell NativeEdge

Wprowadzaj innowacje, gdziekolwiek działasz

Kompleksowe rozwiązanie, które bezpiecznie centralizuje wdrażanie, aranżację i zarządzanie cyklem życia zróżnicowanej infrastruktury i aplikacji na brzegu oraz w rozproszonych centrach przetwarzania danych.

Upraszczaj, optymalizuj i chroń środowiska brzegowe oraz rozproszone centra przetwarzania danych dzięki różnym funkcjom, takim jak automatyczne wdrażanie, bezpieczeństwo modelu „zero trust” i zaawansowana aranżacja obciążeń roboczych. Rozwiązanie NativeEdge wykorzystuje monitor maszyny wirtualnej KVM i środowisko uruchomieniowe kontenerów, umożliwiając organizacjom wdrażanie maszyn wirtualnych i kontenerów oraz zarządzanie nimi. Jest zoptymalizowane do koordynowania obciążeń roboczych i struktur sztucznej inteligencji, umożliwiając płynne wdrażanie aplikacji opartych na sztucznej inteligencji i zarządzanie nimi na obrzeżach sieci oraz w rozproszonych centrach przetwarzania danych. NativeEdge może również dostosować się do dowolnego środowiska sprzętowego, obsługując szeroką gamę urządzeń różnego typu — od serwerów Dell PowerEdge po komputery stacjonarne, a także infrastrukturę innych producentów.

Rozwiązanie Dell NativeEdge zostało zaprojektowane z myślą o unikatowych wyzwaniach związanych ze środowiskami rozproszonymi, takimi jak złożoność operacyjna, skalowalność i bezpieczeństwo. Jest to rozwiązanie dostosowane do nowoczesnych organizacji, które koncentrują się na wykorzystaniu mocy przetwarzania brzegowego przy jednoczesnym obniżeniu kosztów i zwiększeniu wydajności.

Uproszczenie

Przyspiesz wyniki i scentralizuj operacje

Mniej niż
1 minuta
na wdrożenie infrastruktury i aplikacji[1]

Optymalizacja

Osiągnij płynną wirtualizację i skalowalną sztuczną inteligencję

Nawet
68%
oszczędności czasu dzięki automatyzacji aranżacji aplikacji brzegowych[1]

Ochrona

Pracuj bez obaw dzięki modelowi bezpieczeństwa zero-trust

Włącz
najbezpieczniejsze
na świecie operacje brzegowe[2]

[1] Zatwierdzenie techniczne Enterprise Strategy Group firmy TechTarget zlecone przez firmę Dell Technologies, „Dell NativeEdge Edge Operations Software Platform”, luty 2025 r.

[2] Na podstawie analizy wewnętrznej przeprowadzonej przez firmę Dell Technologies, maj 2025 r.

Dell.com/NativeEdge

Zabezpiecz swoją rozbudowującą się infrastrukturę rozproszoną poprzez ciągłe i automatyczne wzmacnianie bezpieczeństwa infrastruktury, aplikacji, danych, sieci i użytkowników bez konieczności interwencji działu IT.

Dell NativeEdge chroni operacje rozproszone poprzez

Wzmocnienie bezpieczeństwa opartego na modelu „zero-trust”

Nowoczesne przedsiębiorstwa są odpowiedzialne za zarządzanie tysiącami aplikacji w rozproszonych geograficznie lokalizacjach i często opierają się na heterogenicznej infrastrukturze. Tworzy to złożoną sieć silosów technologicznych, które są nieefektywne w zarządzaniu, trudne do zabezpieczenia i powolne w aktualizacji. W miarę jak organizacje wdrażają nowe aplikacje, czujniki i urządzenia w rozproszonych lokalizacjach, powierzchnia ataku dla potencjalnych zagrożeń cybernetycznych rośnie.

W jaki sposób przedsiębiorstwa mogą zapewnić ciągłe bezpieczeństwo operacji związanych z danymi rozproszonymi?

Dell NativeEdge umożliwia bezpieczne działanie dzięki modelowi bezpieczeństwa typu „zero trust”. Od momentu włączenia urządzenia tworzony jest łańcuch zaufania oparty na sprzęcie, wykorzystujący funkcje takie jak UEFI Secure Boot i wirtualny moduł Trusted Platform Module (vTPM) w celu zapewnienia integralności urządzenia. Dzięki zintegrowanej obsłudze RODO i innych globalnych wymogów dotyczących suwerenności danych NativeEdge zapewnia spokój ducha w środowiskach rozproszonych. Takie podejście, w połączeniu z funkcjami takimi jak mikrosegmentacja oparta na modelu „zero-trust”, chroni aplikacje i dane, umożliwiając bezpieczne wprowadzanie innowacji niezależnie od miejsca działania.

Model bezpieczeństwa zero-trust

Poziom bezpieczeństwa jest dodatkowo wzmocniony dzięki monitorowaniu i zrozumieniu wszystkich działań zasobów, co jest możliwe dzięki odpowiednim kontrolom biznesowym, scentralizowanej płaszczyźnie kontroli oraz infrastrukturze, która wyraźnie działa w tym zakresie. Dzięki zasadom projektowania w modelu „zero trust" NativeEdge przedsiębiorstwa mogą mieć pewność, że w miarę rozszerzania rozproszonych operacji integralność wszystkich połączonych zasobów jest stale weryfikowana i zatwierdzana.

Zapewnienie integralności sprzętu w całym łańcuchu dostaw i cyklu eksploatacji produktu

Patrząc na przykłady detalistów lub producentów mających sklepy lub fabryki na całym świecie, coraz trudniej jest zarządzać różnorodnym sprzętem o różnych specyfikacjach i profilach w zależności od lokalizacji oraz zapewnić jego bezpieczeństwo. Z biegiem czasu urządzenia te nie są stale certyfikowane, a zgodność z przepisami nie może być weryfikowana w dłuższej perspektywie czasowej. Ryzyko to rośnie gwałtownie, gdy w instalacji tych urządzeń bierze udział wiele stron.

Jak można konsekwentnie chronić infrastrukturę rozproszoną?

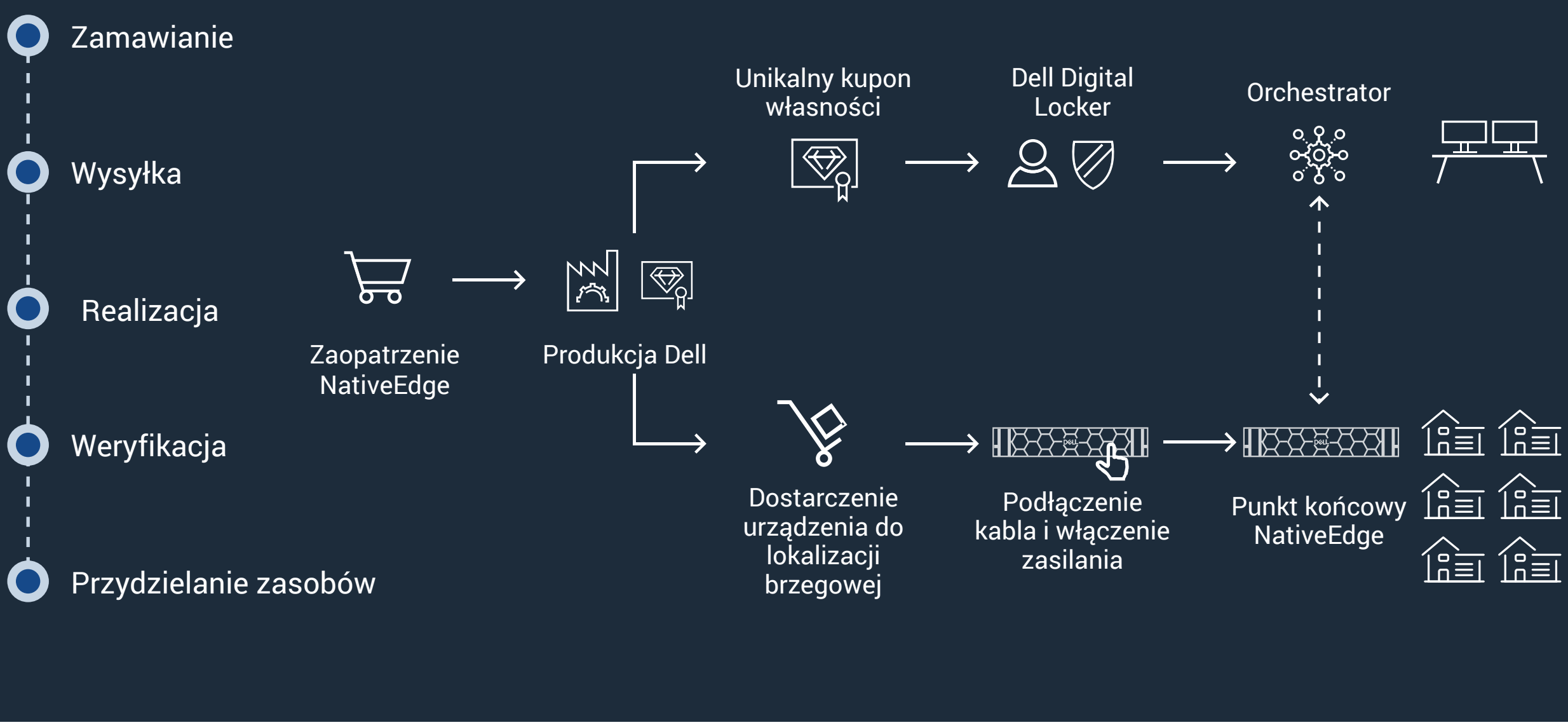
Ochrona infrastruktury zaczyna się w naszej fabryce. Urządzenia końcowe NativeEdge są chronione za pomocą zabezpieczeń kryptograficznych i funkcji Secured Component Verification (SCV) w celu zapewnienia autentyczności. Umożliwia to bezpieczny proces wdrażania bez konieczności interwencji użytkownika przy użyciu wdrażania urządzeń opartemu na FIDO (FDO). Po włączeniu urządzenia w dowolnej lokalizacji jego integralność jest automatycznie weryfikowana, co pozwala ustanowić bezpieczny łańcuch nadzoru bez konieczności ręcznej interwencji. Dzięki temu można skalować działalność, mając pewność, że infrastruktura jest bezpieczna od pierwszego dnia.

Urządzenia końcowe NativeEdge są zoptymalizowane pod kątem zgodności z NativeEdge i chronione zabezpieczeniami kryptograficznymi w fabryce Dell.

NativeEdge wykorzystuje proces Secured Component Verification (SCV) w celu zapewnienia autentyczności i integralności komponentów sprzętowych. Dzięki SCV NativeEdge gwarantuje integralność łańcucha dostaw, weryfikację komponentów, walidację oprogramowania układowego, bezpieczne procesy rozruchu i podpisy kryptograficzne w celu ochrony przed nieautoryzowanym dostępem lub manipulacją.

Ponieważ urządzenia te przechodzą proces wdrażania oparty na standardzie FIDO, ich integralność jest automatycznie certyfikowana, co zapewnia bezpieczeństwo od momentu produkcji w fabryce Dell aż po odbiór i instalację w miejscu wdrożenia. Jeśli sprzęt zostanie w jakikolwiek sposób zmodyfikowany, platforma automatycznie izoluje go, chroniąc operacje przed niepożądanymi elementami.

Wdrażanie urządzeń zabezpieczających i struktura modelu „zero trust”

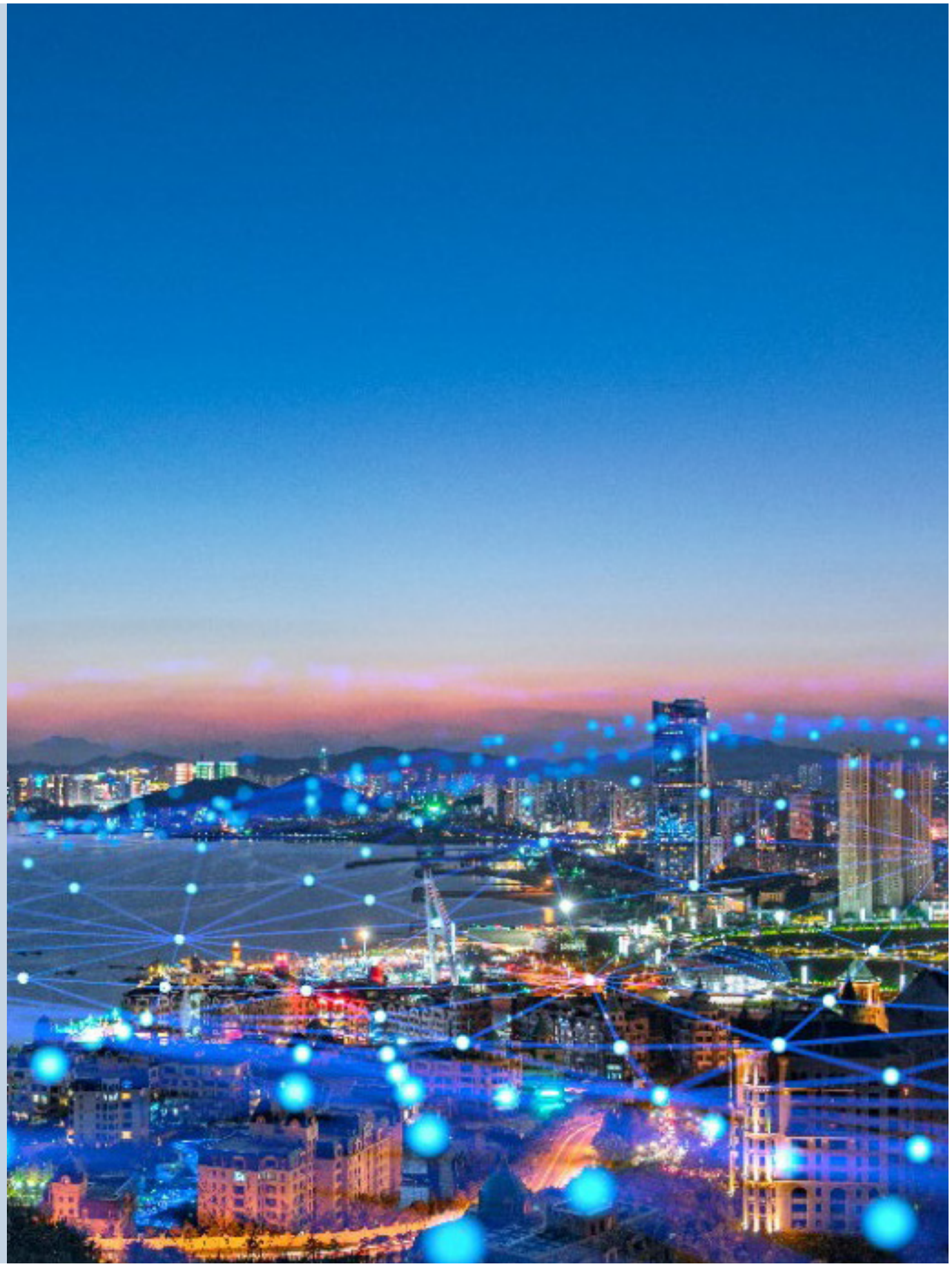


Wzmacnianie danych i aplikacji od obrzeża sieci do chmury

Rozważmy przykład globalnego detalisty. Zróżnicowany i rozproszony charakter środowisk detalicznych oznacza, że tożsamość użytkowników uzyskujących dostęp do aplikacji i obciążeń roboczych może nie być rutynowo weryfikowana. Jeśli tak się dzieje, odbywa się to lokalnie w danym środowisku i nie jest widoczne ani kontrolowane centralnie.

Ponadto sprzedawcy detaliczni rzadko mają wgląd w łańcuch dostaw oprogramowania wdrożonych aplikacji. Często zajmują się tym dostawcy usług zarządzanych (MSP) i może nie być żadnych widocznych automatycznych kontroli zgodności tych aplikacji. Aplikacje te są często początkowo konfigurowane przez tych samych dostawców usług zarządzanych, co może powodować zmiany konfiguracji w miarę upływu czasu. W związku z tym interesariusze nie są w stanie określić zgodności aplikacji z politykami bezpieczeństwa.

W przypadku producentów zespół ds. technologii operacyjnej (OT) zazwyczaj obsługuje różnorodny zestaw obciążeń aplikacji. Niektóre z tych aplikacji współpracują z urządzeniami takimi jak sterowniki PLC i są aplikacjami zastrzeżonymi, które nie są widoczne wewnętrznie.



Możliwości sieci IT nie są przenoszone do sieci OT, która jest logicznie oddzielona. W rezultacie infrastruktura i obciążenia aplikacji w sieciach OT producentów nie mają dostępu do poziomu kontroli bezpieczeństwa sieciowego niezbędnego do zapewnienia bezpiecznego środowiska OT. Podobne wyzwania związane z bezpieczeństwem aplikacji i danych są powszechne we wszystkich branżach.

Dell NativeEdge pomaga organizacjom zabezpieczyć przepływ danych od źródeł danych do aplikacji działających lokalnie lub w chmurze. Łączy w sobie zaawansowane środki bezpieczeństwa, takie jak szyfrowanie, kontrola dostępu użytkowników, katalog schematów aplikacji, segmentacja sieci i koordynacja bezpieczeństwa. NativeEdge wykorzystuje również telemetrię i analitykę do proaktywnej oceny stanu bezpieczeństwa rozproszonych lokalizacji bez konieczności angażowania ekspertów z uprawnieniami audytorskimi do odwiedzania każdej lokalizacji.

Zaawansowane środki bezpieczeństwa

Zaawansowane środki bezpieczeństwa zapewniają niezawodność działania

Kontrola dostępu użytkowników

NativeEdge zapewnia kontrolę dostępu opartą na rolach (RBAC) w celu analizowania poziomów dostępu w oparciu o role i obowiązki użytkownika. Użytkownicy urządzeń i wdrożonych obciążeń aplikacji są weryfikowani podczas każdej sesji dostępu, a także poświadczani w scentralizowany i widoczny sposób poprzez zarządzanie tożsamością i dostępem.

Segmentacja sieci

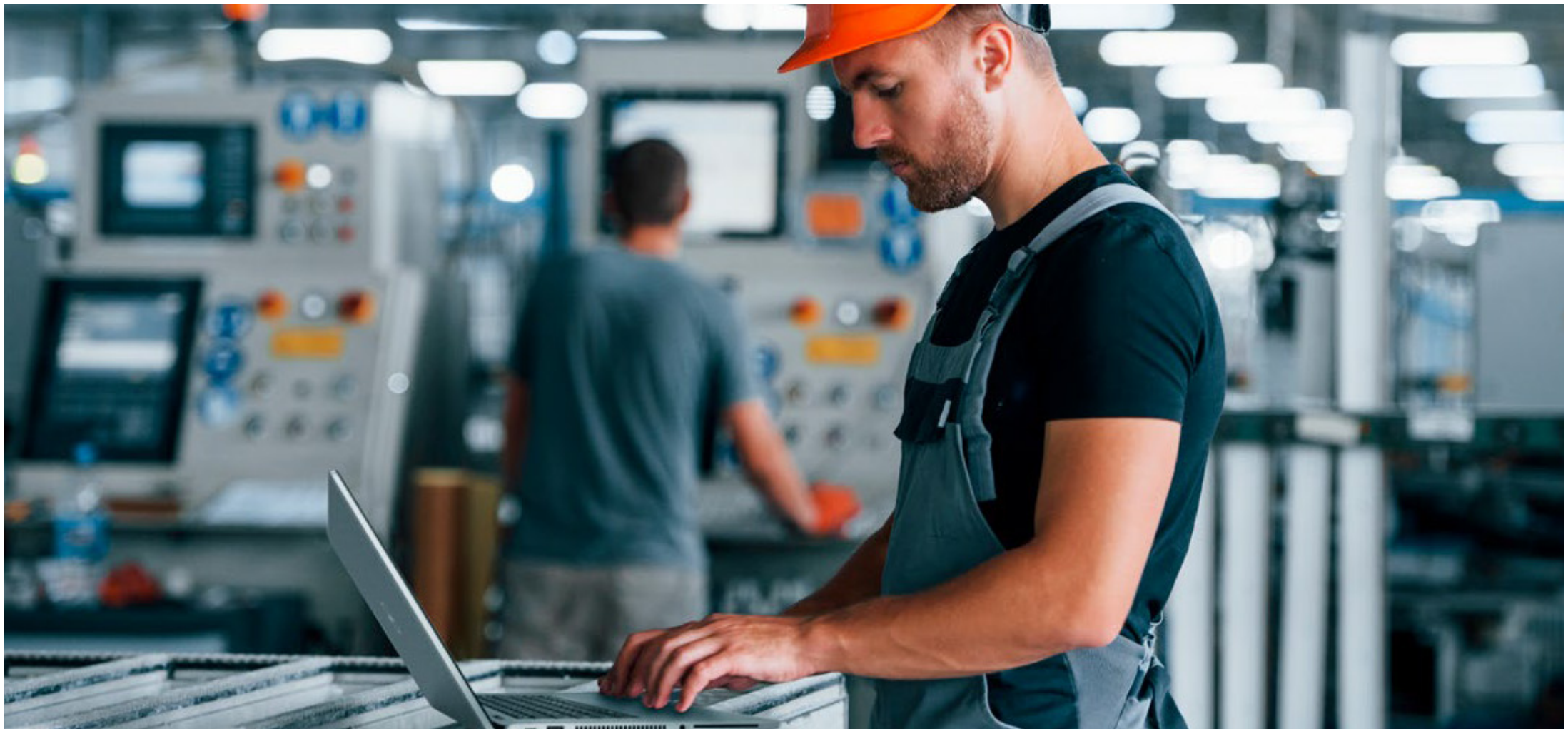
Mikrosegmentacja sieci dla aplikacji ułatwia opracowywanie i zarządzanie zasadami, które są ukierunkowane na te aplikacje, aby zwiększyć ich bezpieczeństwo. Takie podejście ogranicza ryzyko potencjalnych naruszeń i przemieszczania się zagrożeń w środowiskach wirtualnych.

Katalog projektów aplikacji

NativeEdge zostało zaprojektowane w celu zwiększenia bezpieczeństwa aplikacji. Pierwszym krokiem jest bezpieczny łańcuch dostaw oprogramowania, który opiera się na katalogu umożliwiającym wdrażanie aplikacji przy użyciu projektów. Katalog jest zbiorem projektów wdrażania aplikacji od niezależnych dostawców oprogramowania (ISV) lub wstępnie zweryfikowanych projektów firmy Dell opracowanych przez przedsiębiorstwa, a wszystko to w celu utrzymania bezpiecznego łańcucha dostaw oprogramowania. Te projekty, oparte na standardzie TOSCA i formacie YAML, automatyzują wdrażanie aplikacji, a także struktur SI na wielu urządzeniach brzegowych jednocześnie. NativeEdge umożliwia ustawienie proaktywnych kontroli bezpieczeństwa dla wdrożonych aplikacji na poziomie szczegółowym i zapewnia, że aplikacje są wdrażane spójnie i zgodnie z polityką bezpieczeństwa. Podsumowując, obciążenia aplikacji mogą być uruchamiane na punktach końcowych NativeEdge lub w środowisku wielu chmur jako maszyny wirtualne i kontenery, zarządzane centralnie przez NativeEdge.

Szyfrowanie i ochrona danych

NativeEdge chroni dane niezależnie od tego, gdzie się znajdują — w stanie spoczynku, w trakcie przesyłania czy podczas użytkowania — przed naruszeniami i nieautoryzowanym dostępem. NativeEdge zapewnia solidne szyfrowanie danych w stanie spoczynku (DARE), które spełnia federalne standardy zgodności, gwarantując, że przechowywane dane są szyfrowane i chronione przed fizyczną kradzieżą lub manipulacją. NativeEdge zarządza wszystkimi zasobami danych zgodnie z zasadami bezpieczeństwa modelu „zero-trust”, egzekwując ścisłą kontrolę dostępu oraz stale poświadczając i weryfikując kontrolę dostępu. Nie tylko chroni to integralność danych w aplikacjach korporacyjnych, ale także zwiększa zaufanie wszystkich interesariuszy biznesowych.



Koordynacja zabezpieczeń

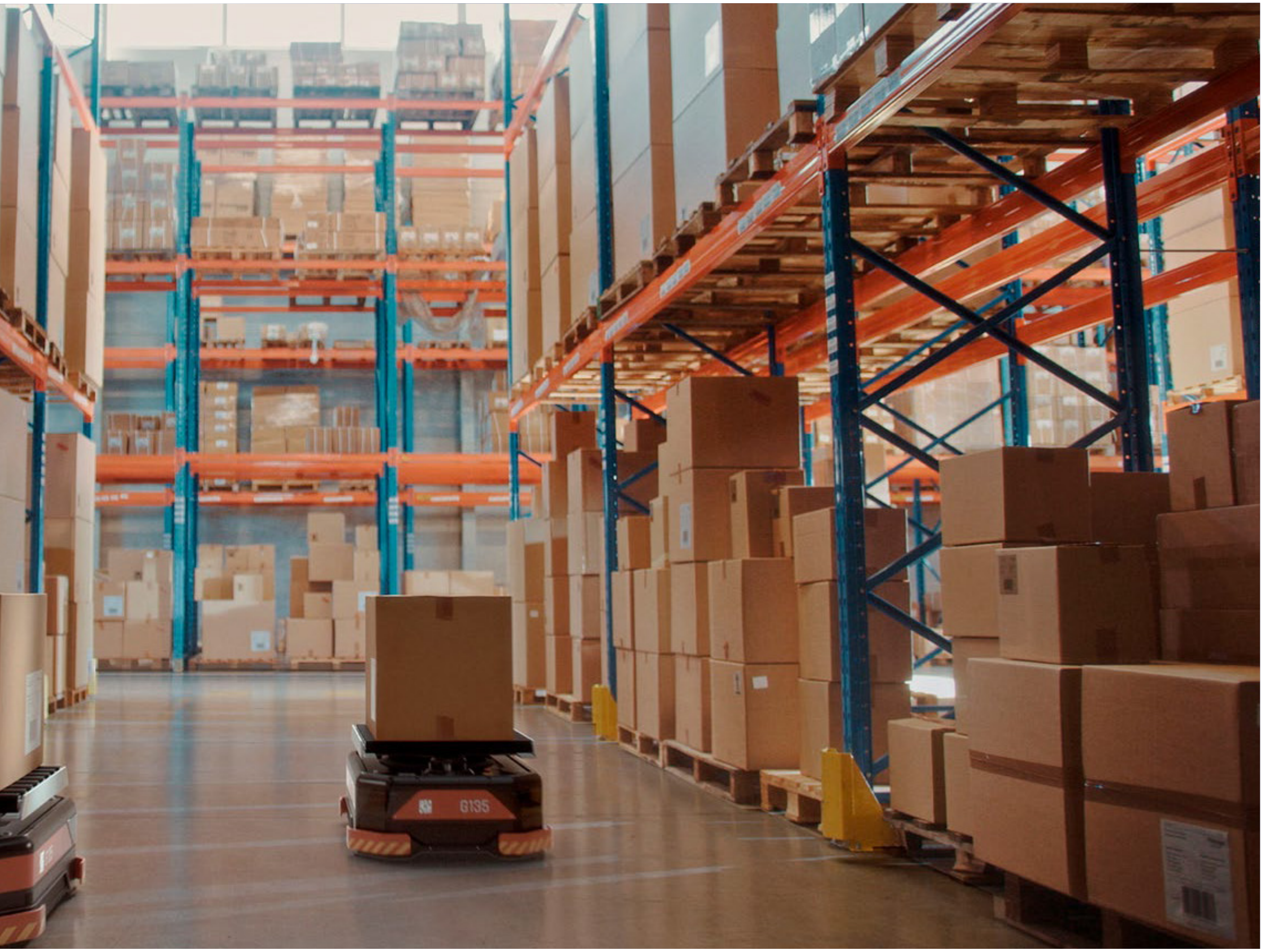
Nieautoryzowane działania/zdarzenia często pozostają niezauważone i często nigdy nie są naprawiane. Prowadzi to do powstania ryzyka z powodu ręcznych procesów i często schodzi na dalszy plan wobec priorytetowych zadań biznesowych. Ponadto istnieją różnice w integracji IT w zakresie zarządzania tożsamością i dostępem (IAM) / kontroli dostępu opartej na rolach (RBAC) oraz płaszczyzny kontroli.

Prowadzi to do rozłącznej koordynacji bezpieczeństwa, która często jest zarządzana indywidualnie w każdej lokalizacji. W wielu przypadkach OT urządzenia te znajdują się w środowisku technologii Machine-to-Machine (M2M), które nie ma świadomości użytkownika. Scentralizowana koordynacja ma kluczowe znaczenie dla tych środowisk.

NativeEdge zapewnia spójną koordynację bezpieczeństwa w całej infrastrukturze brzegowej. Na podstawie zbioru działań i zdarzeń, które mają miejsce w środowisku brzegowym, rozwiązanie to zapewnia ujednolicony obraz stanu bezpieczeństwa, umożliwiając scentralizowane uwierzytelnianie i spójne egzekwowanie zasad we wszystkich lokalizacjach. Wykorzystuje funkcje IAM i RBAC, które umożliwiają bezpieczne zarządzanie platformą przy użyciu zasady minimalnych uprawnień, zapewniając w ten sposób szczegółowość, której potrzebują przedsiębiorstwa. Rozwiązanie NativeEdge upraszcza również zachowanie zgodności z przepisami, takimi jak RODO, PCI i HIPAA, poprzez automatyzację rejestrowania i zarządzania konfiguracją, pomagając w pewnym działaniu w każdym środowisku dzięki możliwości włączenia zasad z zakresu zarządzania, ryzyka i zgodności (GRC) / operacji zabezpieczeń (SecOps).

Telemetria i analityka

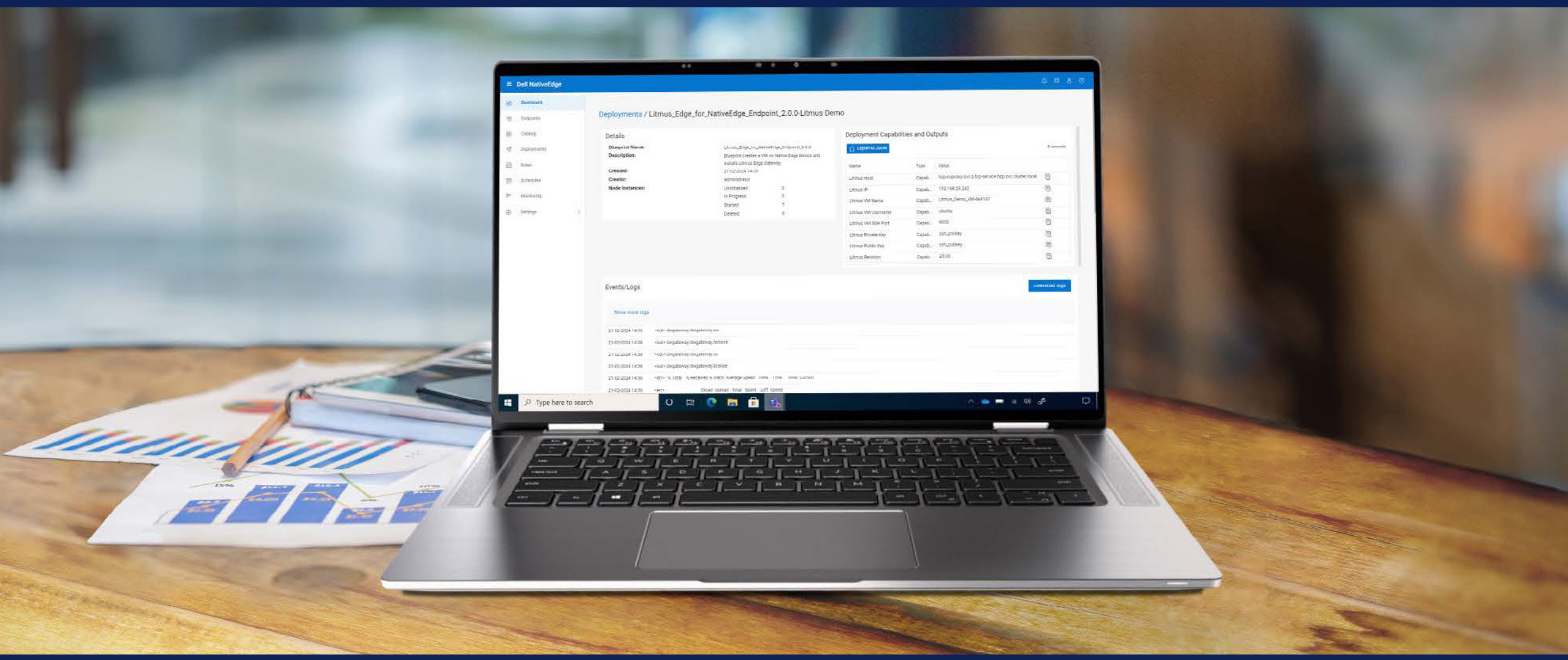
NativeEdge nieustannie przeprowadza oceny bezpieczeństwa zgodnie z określonymi standardami zgodności, opierając się na danych telemetrycznych pochodzących ze sprzętu i środowiska operacyjnego. Są one wykorzystywane do wykrywania odchyleń konfiguracyjnych, błędnych konfiguracji i konieczności aktualizacji zabezpieczeń.



Chroń swoją infrastrukturę brzegową

Dell NativeEdge chroni Twoją infrastrukturę brzegową dzięki modelowi bezpieczeństwa „zero trust”, w tym bezpiecznemu wdrażaniu urządzeń opartych na FIDO oraz wzmocnionemu i bezpiecznemu systemowi operacyjnemu NativeEdge. Dzięki Dell NativeEdge możesz mieć pewność, że Twoja infrastruktura, użytkownicy, sieć, aplikacje i dane są stale weryfikowane i sprawdzane we wszystkich lokalizacjach.

Wprowadzaj innowacje, gdziekolwiek działasz



DELL Technologies

Więcej informacji o **Dell.com/NativeEdge**