Dell NativeEdge

보호: 제로 트러스트 보안으로 안심하고 운영

표:

목차

분산 환경 전반의 보안

급변하는 고객 선호도와 시장 역학에 대응하기 위해 조직들은 전례 없는 규모와 속도로 새로운 애플리케이션, 업데이트 및 컴퓨팅 인프라스트럭처를 배포하고 있습니다. 이처럼 데이터, 인프라스트럭처 및 애플리케이션이 쏟아져 나오면서 이러한 신기술이 존재하는 분산 환경을 보호하는 것이 점점 더 중요해지고

있습니다. 기업이 운영을 확장함에 따라 물리적 디바이스 변조부터 데이터

해킹에 이르기까지 다양한 보안 위험에 더욱 취약해집니다. 또한 이러한 시스템은 종종 민감한 개인 데이터를 처리하므로 기업에서 고객을 보호해야 할 책임은 더욱 커집니다.

기업은 운영 보안을 유지하기 위해 다음과 같은 조치를 취해야 합니다.

분산된 위치에 배포된
인프라스트럭처의 물리적 안전
확보

디바이스 변조
탐지 및 위협
해결

모든 단계에서
사용자 접근
제어

수천 대의 디바이스에 걸쳐 프로비저닝
및 소프트웨어 업데이트
확장

Dell NativeEdge

가능한 모든 곳에서 혁신 실현

엣지 및 분산 데이터 센터 전반에서 다양한 인프라스트럭처와 애플리케이션의 배포, 오케스트레이션 및 수명주기 관리를 안전하게 중앙 집중화하는 포괄적인 풀 스택 솔루션입니다.

제로 터치 온보딩, 제로 트러스트 보안, 고급 워크로드 오케스트레이션과 같은 기능으로 엣지 및 분산 데이터 센터 환경을 간소화, 최적화 및 보호합니다. NativeEdge는 KVM 하이퍼바이저 및 컨테이너 런타임을 활용하여 조직에서 VM(Virtual Machine)과 컨테이너를 모두 배포하고 관리할 수 있도록 합니다. AI 워크로드 및 프레임워크 오케스트레이션에 최적화되어 있어 엣지 및 분산 데이터 센터 전반에 걸쳐 AI 기반 애플리케이션을 원활하게 배포하고 관리할 수 있습니다. 또한 NativeEdge는 Dell PowerEdge 서버부터 데스크탑, 타사 인프라스트럭처에 이르기까지 다양한 폼 팩터의 광범위한 옵션을 지원하여 모든 하드웨어 환경에 적응할 수 있습니다.

Dell NativeEdge는 운영 복잡성, 확장성, 보안과 같은 분산 환경의 고유한 문제를 해결하도록 특별히 설계되었습니다. 비용을 절감하고 효율성을 향상하면서 엣지 컴퓨팅의 강력한 기능을 활용하는 데 중점을 둔 현대 조직에 최적화된 솔루션입니다.

간소화
성과 가속화 및 운영 중앙 집중화

소요 시간
1분
미만으로 인프라스트럭처 및 애플리케이션 배포[1]

최적화
원활한 가상화와 확장 가능한 AI 실현

엣지 애플리케이션 오케스트레이션을 자동화하여 최대
68%
시간 절약[1]

보호
제로 트러스트 보안으로 안심하고 운영

세계적
수준의 보안
엣지 운영 지원[2]

[1] Dell Technologies의 의뢰로 TechTarget의 Enterprise Strategy Group에서 수행한 기술적 유효성 검사, "Dell NativeEdge Edge Operations Software Platform", 2025년 2월.

[2] Dell Technologies 내부 분석 기준, 2025년 5월.

Dell.com/NativeEdge

IT 부서의 개입 없이 인프라스트럭처, 애플리케이션, 데이터, 네트워크 및 사용자 보안을 지속적이고 자동으로 강화하여 확장되는 분산 운영의 보안을 유지하십시오.

Dell NativeEdge의 분산 운영 보호 방식

제로 트러스트 보안 강화

현대 기업들은 지리적으로 분산된 여러 사이트에 걸쳐 수천 개의 애플리케이션을 관리해야 하며, 종종 이기종 인프라스트럭처 조합에 의존합니다. 이로 인해 관리 효율성이 떨어지고 보안이 취약하며 업데이트 속도가 느린 복잡한 기술 사일로 웹이 발생합니다. 조직들이 분산된 위치에 새로운 애플리케이션, 센서 및 디바이스를 계속해서 배포함에 따라 잠재적인 사이버 위협에 대한 공격 노출 지점도 증가합니다.

기업은 어떻게 분산 데이터 운영의 지속적인 보안을 보장할 수 있습니까?

Dell NativeEdge는 제로 트러스트 보안을 기반으로 안심하고 운영할 수 있도록 지원합니다. 디바이스 전원이 켜지는 순간부터 UEFI 보안 부팅 및 vTPM(virtual Trusted Platform Module)과 같은 기능을 활용해 하드웨어 기반의 신뢰 체인이 구축되어 디바이스 무결성을 보장합니다. GDPR 및 기타 글로벌 데이터 주권 의무 사항을 기본적으로 지원하는 NativeEdge는 분산 환경에 대한 안심할 수 있게 해줍니다. 이러한 접근 방식은 제로 트러스트 마이크로 세분화와 같은 기능과 결합되어 애플리케이션과 데이터를 보호하므로 어디에서 운영하든 안전하게 혁신할 수 있습니다.

제로 트러스트(Zero-trust) 보안

관련 비즈니스 제어, 중앙 집중식 제어 플레인, 그리고 이를 위해 명시적으로 작동하는 인프라스트럭처를 통해 리소스의 모든 활동을 모니터링하고 파악함으로써 보안 태세를 더욱 강화할 수 있습니다. NativeEdge의 제로 트러스트 설계 원칙을 통해 기업은 분산 운영이 확장됨에 따라 연결된 모든 리소스의 무결성이 지속적으로 인증되고 확인된다는 것을 확신할 수 있습니다.

공급망 및 수명주기 전반에 걸쳐 하드웨어 무결성 보장

전 세계에 매장이나 공장을 보유한 소매업체 또는 제조업체의 경우, 위치에 따라 사양과 프로파일이 다른 다양한 하드웨어를 관리하고 보호하는 것이 점점 더 어려워집니다. 시간이 지남에 따라 이러한 디바이스에 대한 지속적인 인증이 이루어지지 않고, 장기간에 걸쳐 규정 준수 여부를 확인할 수 없습니다. 이러한 디바이스 설치에 여러 당사자가 관여하는 경우 이러한 위험은 기하급수적으로 증가합니다.

분산된 인프라스트럭처를 어떻게 일관되게 보호할 수 있습니까?

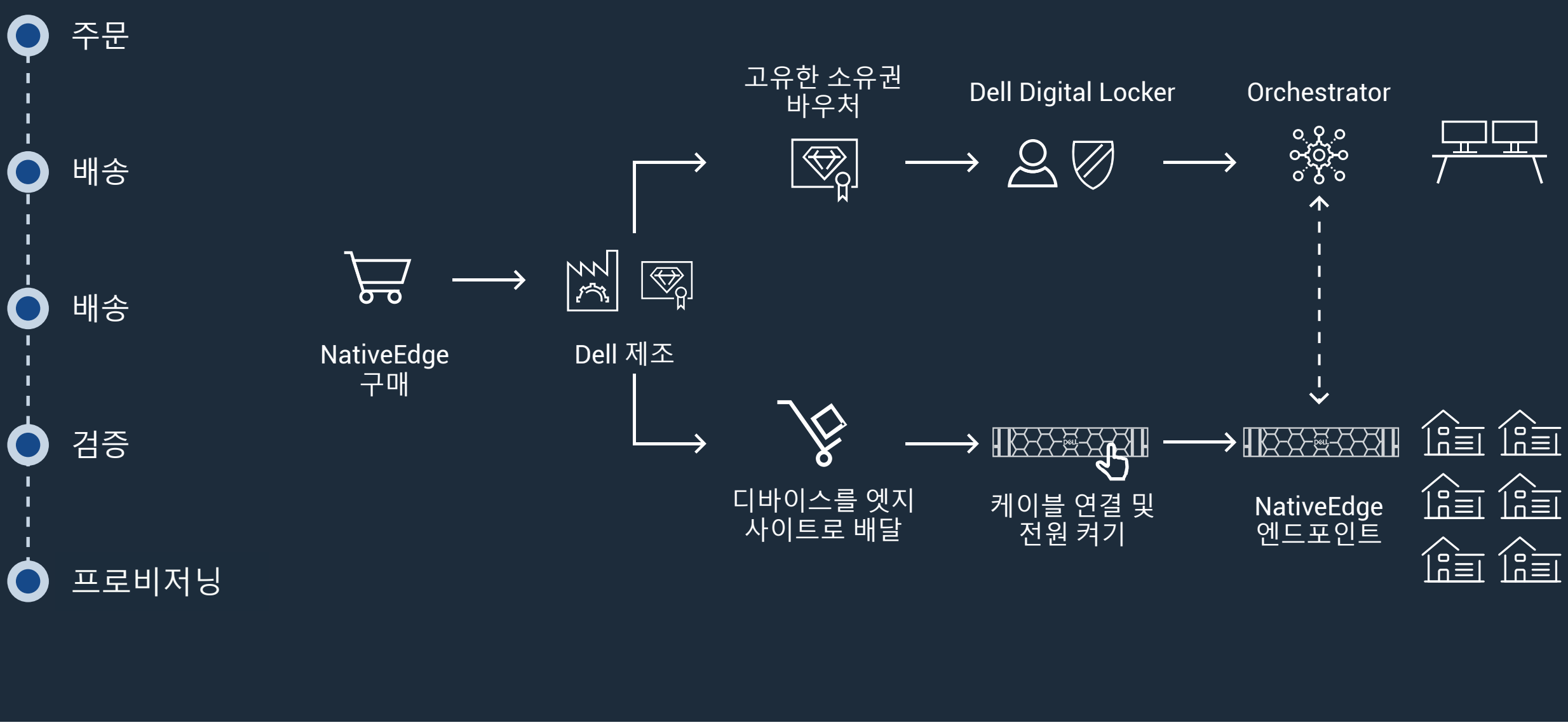
인프라스트럭처 보호는 Dell Technologies 공장에서 시작됩니다. NativeEdge 엔드포인트는 암호화 보안과 SCV(Secured Component Verification)로 보호되어 신뢰성을 보장합니다. 이를 통해 FDO(FIDO Device Onboarding)를 활용한 안전한 제로 터치 배포 프로세스가 이루어질 수 있습니다. 어느 위치에서든 디바이스 전원을 켜면 자동으로 무결성이 검증되어 수동 개입 없이 안전한 관리 체계가 구축됩니다. 따라서 처음부터 인프라스트럭처가 안전하다는 확신을 가지고 운영 규모를 확장할 수 있습니다.

NativeEdge 엔드포인트는 NativeEdge와의 호환성에 최적화되었으며 Dell 공장에서 암호화 보안으로 보호됩니다.

NativeEdge는 SCV(Secured Component Verification) 프로세스를 활용하여 하드웨어 구성 요소의 신뢰성과 무결성을 보장합니다. NativeEdge는 SCV를 통해 공급망 무결성, 구성 요소 검증, 펌웨어 유효성 검사, 보안 부팅 프로세스 및 암호화 서명을 적용하여 무단 액세스 또는 변조로부터 보호합니다.

이러한 디바이스는 FIDO 기반 디바이스 온보딩 프로세스를 거치면서 무결성이 자동으로 인증되므로 Dell 공장에서의 제조부터 배포 현장에서의 수령 및 설치에 이르기까지 보안이 보장됩니다. 하드웨어가 어떤 방식으로든 변조될 경우 플랫폼은 자동으로 해당 하드웨어를 격리하여 악성 요소로부터 운영을 보호합니다.

안전한 디바이스 온보딩과 제로 트러스트 프레임워크

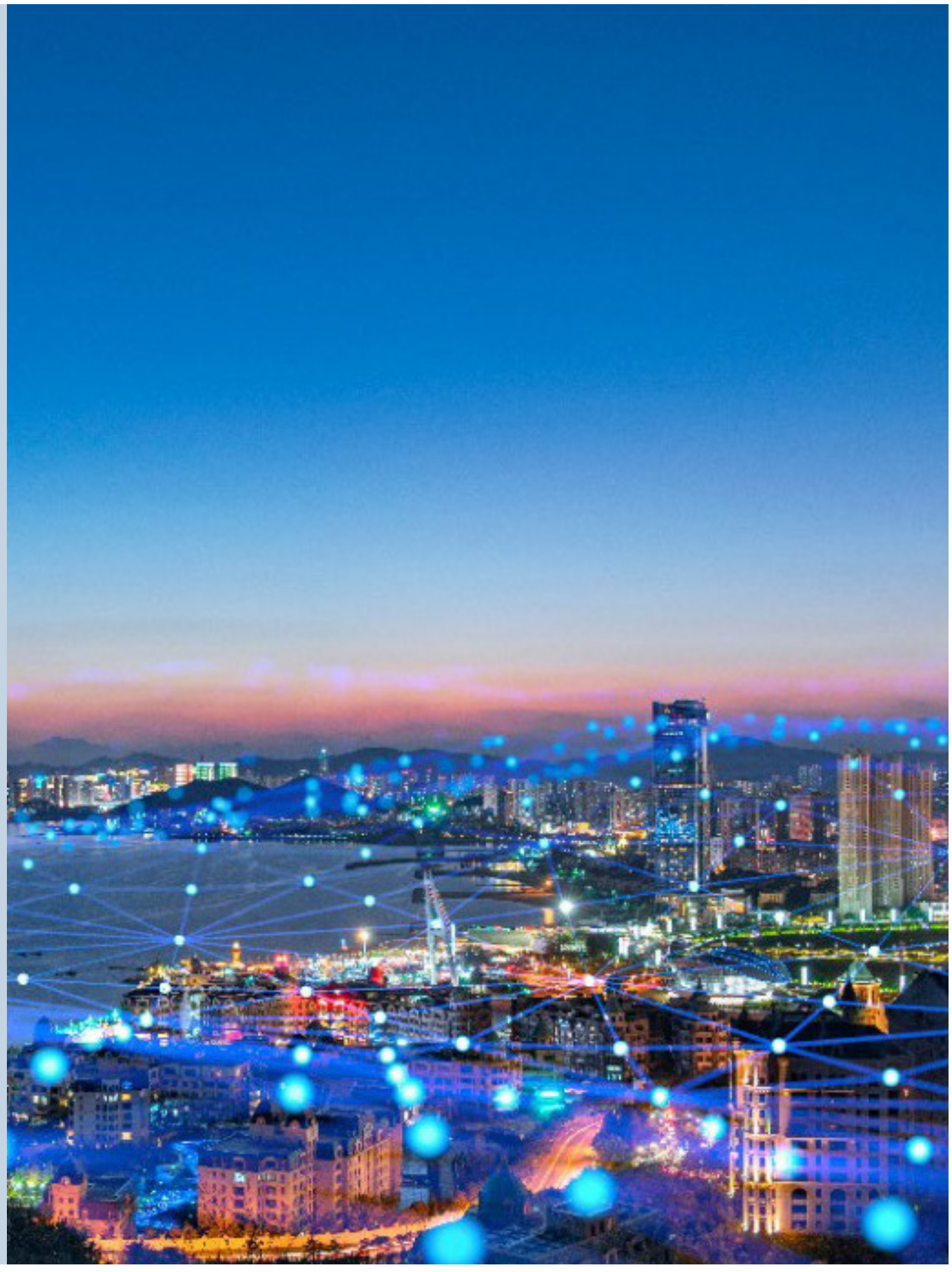


엣지에서 클라우드까지 데이터와 애플리케이션 강화

글로벌 소매업체의 사례를 생각해 보겠습니다. 소매 환경은 다양하고 분산되어 있기 때문에 애플리케이션과 워크로드에 접근하는 사용자의 신원을 정례적으로 검증하기 어려울 수 있습니다. 검증이 이루어진다 하더라도 해당 환경에만 국한되어 중앙에서 확인 및 감사가 불가능합니다.

또한 소매업체는 배포된 애플리케이션의 소프트웨어 공급망을 파악하기 어려운 경우가 많습니다. 이러한 애플리케이션은 주로 MSP(Managed Service Provider)에서 관리하며, 앱의 정확성을 자동으로 검사하는 시스템이 없을 수 있습니다. 이러한 애플리케이션은 초기 구성 시 동일한 MSP에서 담당하는 경우가 많으며, 시간이 지남에 따라 구성이 변경될 가능성이 있습니다. 따라서 이해 관계자는 애플리케이션의 보안 정책 준수 여부를 확인할 수 없습니다.

제조업체의 경우, OT(Operations Technology) 팀이 일반적으로 다양한 애플리케이션 워크로드를 운영합니다. 이러한 애플리케이션 중 일부는 PLC와 같은 장비와 연동되며, 내부적으로 가시성이 확보되지 않은 독점 애플리케이션입니다.



IT 네트워크 기능은 논리적으로 분리된 OT 네트워크로 전달되지 않습니다. 그 결과는, 제조업체의 OT 네트워크 내 인프라스트럭처 및 애플리케이션 워크로드가 안전한 OT 환경을 조성하는 데 필요한 수준의 네트워크 보안 제어에 접근할 수 없다는 것입니다. 이러한 애플리케이션 및 데이터 보안 관련 문제는 모든 산업 분야에서 공통적으로 발생합니다.

Dell NativeEdge는 조직이 데이터 소스에서 로컬 또는 클라우드에서 실행되는 애플리케이션에 이르기까지 데이터 파이프라인을 안전하게 보호할 수 있도록 지원합니다. 암호화, 사용자 액세스 제어, 애플리케이션 청사진 카탈로그, 네트워크 세분화 및 보안 오케스트레이션과 같은 고급 보안 조치를 결합합니다. 또한 NativeEdge는 텔레메트리 및 분석을 활용하여 감사 기능을 갖춘 전문가가 모든 사이트를 직접 방문하지 않고도 분산된 위치의 보안 태세를 사전 예방적으로 평가할 수 있습니다.

고급 보안 조치

고급 보안 조치로 회복탄력성이 뛰어난 운영 보장

사용자 액세스 제어

NativeEdge는 사용자의 역할과 책임에 따라 액세스 수준을 구분하는 RBAC(Role-Based Access Control)를 제공합니다. 디바이스 및 배포된 애플리케이션 워크로드의 사용자는 액세스 세션별로 검증되며, ID 및 액세스 관리를 통해 중앙 집중식으로 투명하게 인증됩니다.

네트워크 세분화

네트워크를 애플리케이션별로 마이크로 세분화하면 해당 애플리케이션을 대상으로 하는 정책을 개발하고 관리하기가 더 쉬워져 보안을 강화할 수 있습니다. 이러한 접근 방식은 가상화된 환경 내에서 발생할 수 있는 잠재적 침해 및 위협의 내부 이동 위험을 완화합니다.

애플리케이션 청사진 카탈로그

NativeEdge는 애플리케이션 보안을 강화하도록 설계되었습니다. NativeEdge는 카탈로그 기반의 안전한 소프트웨어 공급망에서부터 청사진을 사용하여 애플리케이션을 배포합니다. 이 카탈로그는 ISV(Independent Software Vendor)의 애플리케이션 배포용 청사진 모음이거나, 기업에서 개발한 Dell의 사전 검증된 청사진 모음으로, 모두 안전한 소프트웨어 공급망을 유지하는 데 그 목적이 있습니다. TOSCA 표준 및 YAML 형식을 기반으로 하는 이러한 청사진은 애플리케이션과 AI 프레임워크를 여러 엣지 디바이스에 한 번에 배포하는 과정을 자동화합니다. NativeEdge를 사용하면 배포된 애플리케이션에 대해 세분화된 수준에서 사전 예방적 보안 제어를 설정할 수 있으며, 애플리케이션이 보안 정책에 맞춰 일관되게 배포되도록 보장됩니다. 마지막으로, 애플리케이션 워크로드는 NativeEdge 엔드포인트 또는 멀티클라우드 환경에서 VM 및 컨테이너로 실행될 수 있으며, NativeEdge에서 중앙 집중식으로 관리됩니다.

데이터 암호화 및 보호

NativeEdge는 저장 상태 데이터, 전송 중인 데이터, 사용 중인 데이터 등 데이터가 어디에 있든 침해와 무단 액세스로부터 데이터를 보호합니다. NativeEdge는 연방 규정 준수 표준을 충족하는 강력한 DARE(Data at Rest Encryption)를 제공하여 저장된 데이터가 암호화되고 물리적 도난이나 변조로부터 보호되도록 합니다. NativeEdge는 제로 트러스트 보안 원칙에 따라 모든 데이터 리소스를 관리하여 엄격한 액세스 제어를 시행하며 액세스 제어에 대한 지속적인 검증 및 확인을 수행합니다. 이를 통해 엔터프라이즈 애플리케이션의 데이터 무결성을 보호할 뿐만 아니라 모든 비즈니스 이해 관계자의 신뢰도를 높일 수 있습니다.

보안 오케스트레이션

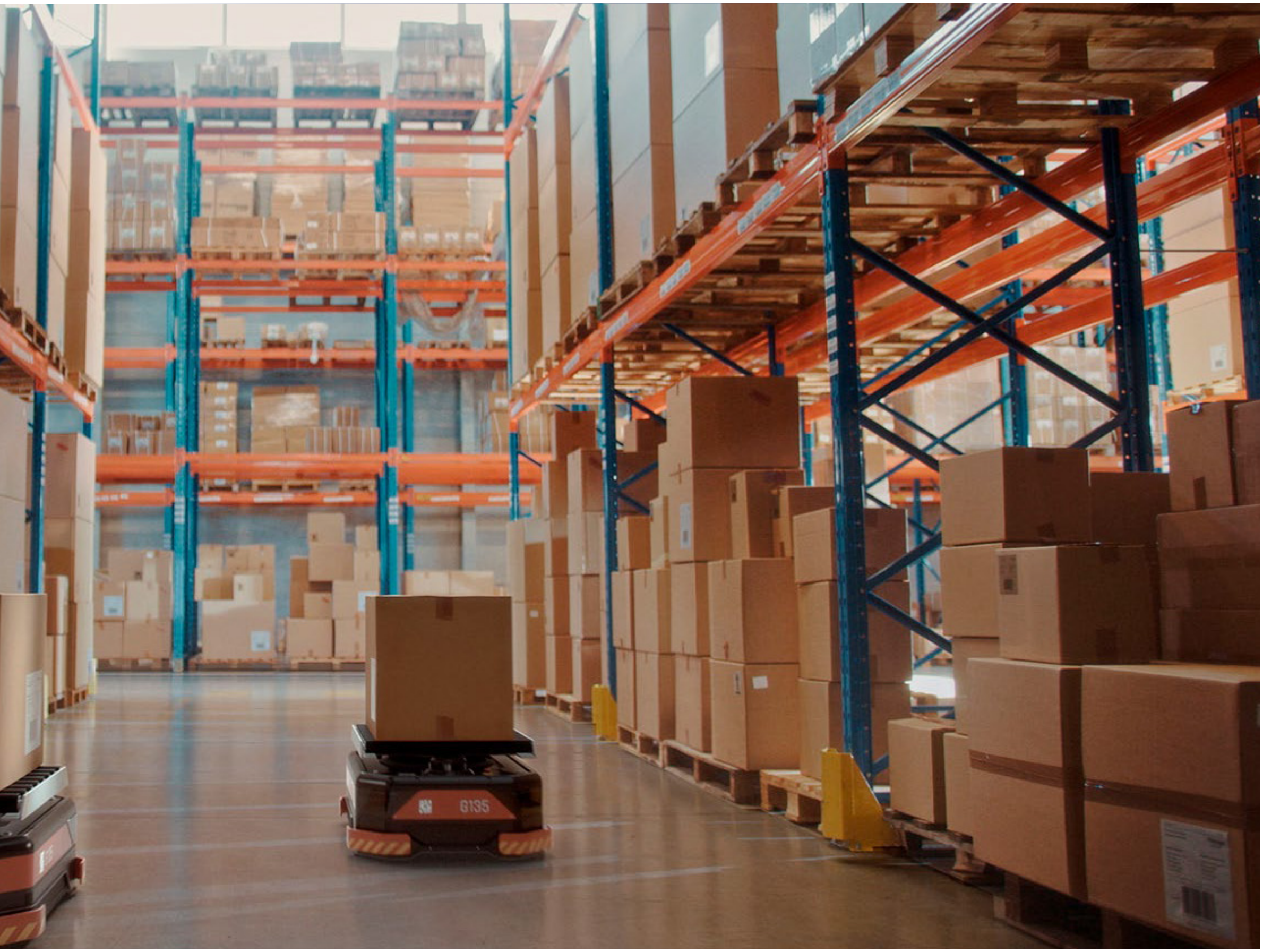
무단 작업/이벤트는 종종 눈에 띄지 않게 발생하며, 해결되지 않는 경우가 많습니다. 이로 인해 수동 프로세스로 위험이 발생하고 우선순위가 높은 비즈니스 작업에 밀려 뒷전으로 미뤄지는 경우가 흔합니다. 또한 IAM(Identity Access Management)/RBAC(Role-Based Access Control) 및 컨트롤 플레인과 관련하여 IT 통합에 편차가 존재합니다.

이는 종종 각 사이트에서 개별적으로 관리되는 단절된 보안 오케스트레이션으로 이어집니다. 많은 OT 사례에서 이러한 디바이스는 사용자 인식이 없는 M2M(Machine-to-Machine) 환경에 있습니다. 이러한 환경에서는 중앙 집중식 오케스트레이션이 매우 중요합니다.

NativeEdge는 엣지 자산 전반에 걸쳐 일관된 보안 오케스트레이션을 보장합니다. 엣지 환경에서 발생하는 작업 및 이벤트의 집계를 기반으로 보안 태세를 통합적으로 파악하여 모든 사이트에서 중앙 집중식 인증과 일관된 정책 적용을 가능하게 합니다. NativeEdge는 최소 권한 원칙에 따라 플랫폼을 안전하게 관리할 수 있는 IAM 및 RBAC 기능을 활용하여 기업에 필요한 세분성을 제공합니다. 또한 NativeEdge는 로깅 및 구성 관리를 자동화하여 GDPR, PCI 및 HIPAA와 같은 규정 준수를 간소화함으로써 GRC(Governance, Risk, and Compliance)/SecOps(Security Operations)의 규칙을 통합할 수 있는 기능을 통해 모든 환경에서 안심하고 운영할 수 있도록 지원합니다.

텔레메트리 및 분석

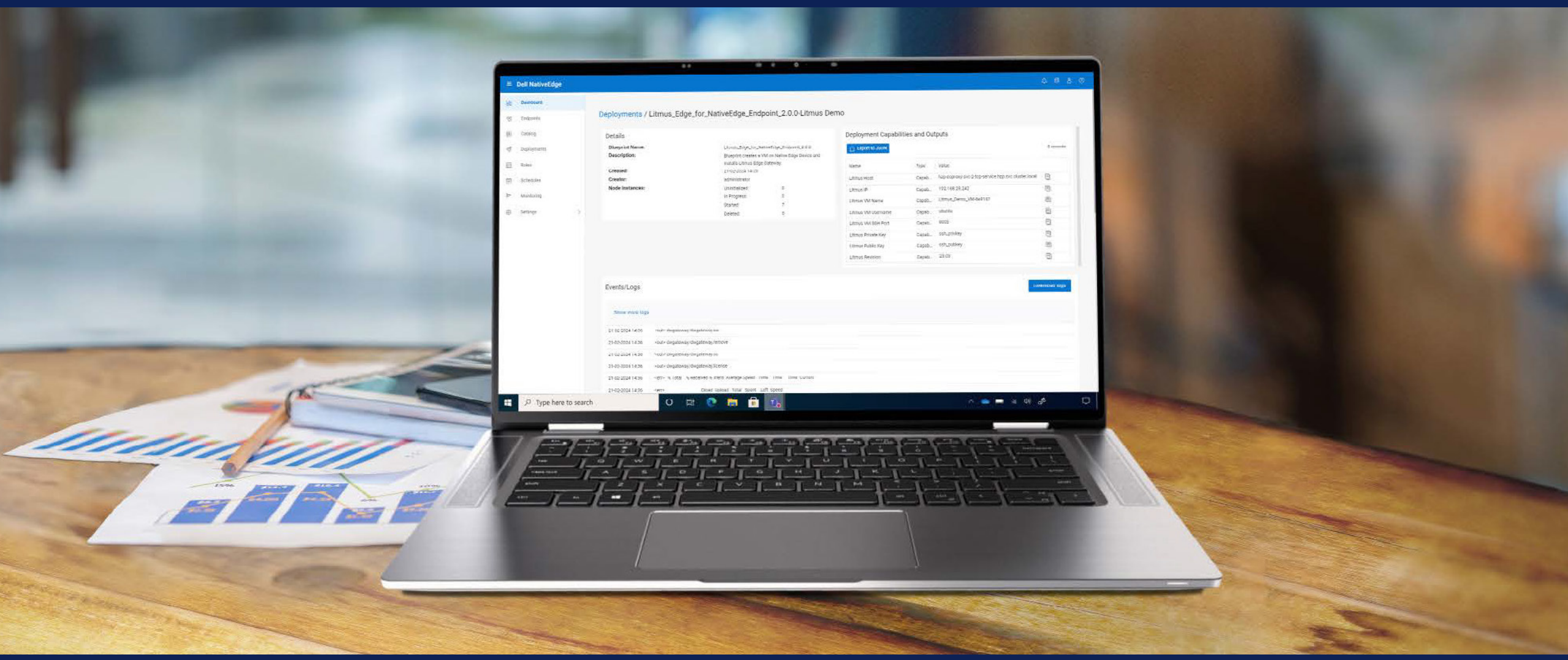
NativeEdge는 하드웨어 및 운영 환경의 텔레메트리를 활용하여 정의된 규정 준수 표준에 따라 지속적으로 보안 평가를 수행합니다. 이러한 평가는 구성 변경 탐지, 잘못된 구성 및 보안 업데이트 필요성을 판단하는 데 사용됩니다.



엣지 자산 보호

Dell NativeEdge는 강화되고 안전한 NativeEdge OS와 결합된 FIDO 기반의 안전한 디바이스 온보딩을 포함한 제로 트러스트 보안 원칙을 통해 엣지 자산을 보호합니다. Dell NativeEdge를 사용하면 분산된 위치 전반에 걸쳐 인프라스트럭처, 사용자, 네트워크, 애플리케이션 및 데이터가 지속적으로 인증되고 확인된다는 것을 확신할 수 있습니다.

가능한 모든 곳에서 혁신 실현



DELL Technologies

Dell.com/NativeEdge에서 자세한 정보 확인