Dell NativeEdge

保护：零信任安全防护，运维无忧

目录

分布式环境中的安全性

为了满足快速变化的客户偏好和市场动态需求，各组织正以前所未有的数量和速度部署新应用程序、更新和计算基础架构。由于数据、基础架构和应用程序的激增，保护这些新技术所在的分布式环境变得越来越重要。

企业在扩展运营时，越来越容易受到安全风险的影响，包括物理设备篡改和数据黑客攻击等。除此之外，这些系统通常会处理敏感的个人数据，因此企业需要承担更多责任来保护其客户。

为确保安全运营，企业需要

确保
部署在分布式位置的
基础架构的物理安全性

检测
设备篡改和
威胁并进行修复

控制
各个级别的
用户访问权限

扩展
数千台设备的资
源调配和软件更新

Dell NativeEdge

随时随地，锐意创新

全堆栈端到端解决方案，可在边缘和分布式数据中心，安全地集中部署、编排各种基础架构和应用程序并进行生命周期管理。

利用零接触接入、零信任安全和高级工作负载编排等功能，简化、优化和保护边缘与分布式数据中心环境。NativeEdge 利用 KVM 虚拟机管理程序和容器运行时，因此组织能够部署和管理虚拟机 (VM) 与容器。它经过优化，可编排 AI 工作负载和框架，从而在边缘和分布式数据中心无缝部署和管理 AI 驱动型应用程序。NativeEdge 还可以适应任何硬件环境，支持各种外形规格的大量选项，包括 Dell PowerEdge 服务器、台式机和第三方基础架构。

Dell NativeEdge 专为解决分布式环境的独特挑战而打造，例如运营复杂性、可扩展性和安全性。该解决方案专为现代组织量身定制，助其充分利用边缘计算的强大功能，同时降低成本并提高效率。

简化
加速成果实现，
集中运维管理

不到
1 分钟
部署基础架构与应用程序的耗时[1]

Optimize
实现无缝虚拟化
并打造可扩展 AI

多达
68%
通过自动执行边缘
应用程序的编排所节省的时间[1]

保护
零信任安全防护，
运维无忧

实现
高度安全的
边缘运维[2]

[1] Dell Technologies 委托 TechTarget 旗下 Enterprise Strategy Group 进行的技术验证，“Dell NativeEdge Edge Operations Software Platform”，2025 年 2 月。

[2] 基于 Dell Technologies 于 2025 年 5 月进行的内部分析。

Dell.com/NativeEdge

通过持续且自动地强化基础架构、应用程序、数据、网络和用户的安全性，妥善保护不断扩展的分布式运营，而无需任何 IT 干预。

Dell NativeEdge 通过以下方式保护分布式运营

强化零信任安全性

现代企业负责管理分布在各地的站点中的数千个应用程序，并且通常依赖于异构基础架构组合。这造成了一个包含多个技术孤岛的复杂网络，管理效率低下、难以确保安全且更新速度缓慢。随着组织不断将新应用程序、新传感器和新设备部署到分布式位置，潜在网络威胁的攻击面不断增加。

企业如何确保分布式数据运营的持续安全性?

Dell NativeEdge 为您打造零信任安全基础，让您放心运营。从设备接通电源的那一刻起，就会建立基于硬件的信任链，利用 UEFI 安全启动和虚拟可信平台模块 (vTPM) 等功能来确保设备完整性。NativeEdge 内置对 GDPR 和其他全球数据主权要求的支持，让您高枕无忧地运营分布式环境。这种方法与零信任微分段等功能相结合，可保护您的应用程序和数据，让您无论在何处运营，都可以安全地进行创新。

零信任安全性

设备信任

用户信任

传输和会话信任

数据信任

软件信任

可见性和分析

自动化和编排

通过监控和了解资源的所有操作，以及在相关业务控制、集中式控制平面和明确自主工作的基础架构的支持下，安全态势得到进一步加强。在 NativeEdge 的零信任设计原则下，企业可以放心，随着分布式运营的扩展，每项连接资源的完整性将持续获得证明与验证。

确保硬件在供应链及其生命周期中的完整性

以拥有全球商店或工厂的零售商或制造商为例，他们越来越难以管理和保护在规格与配置文件上因位置而异的各种硬件。随着时间的推移，这些设备不会持续得到验证，也无法在较长的时间范围内验证合规性。当这些设备的安装涉及多方时，这一风险将呈指数级增长。

如何一致地保护分布式基础架构？

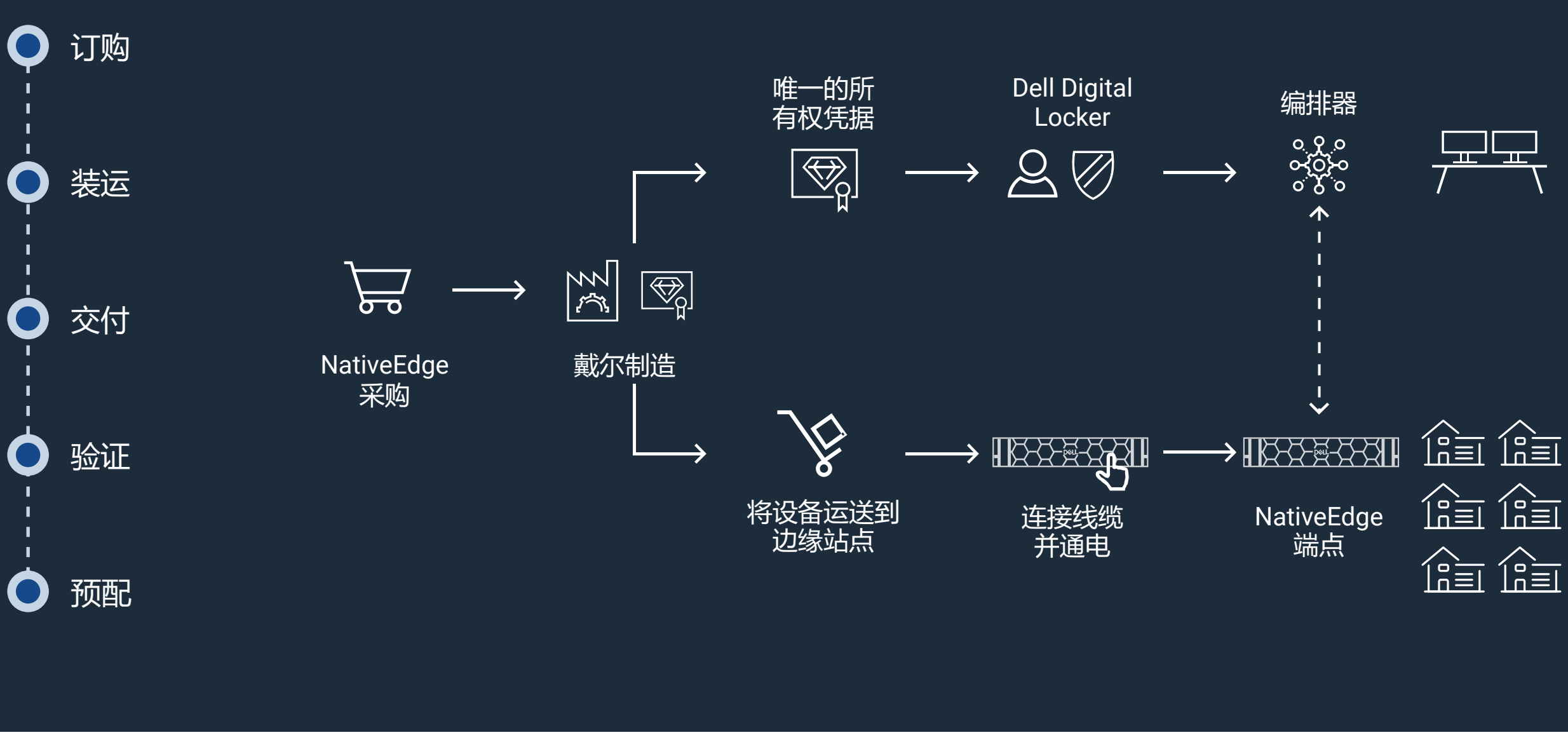
对基础架构的保护始于我们的工厂。NativeEdge 端点受加密安全性和安全组件验证 (SCV) 保护，以确保真实性。因此，使用 FIDO 设备接入 (FDO) 可以实现安全的零接触部署流程。在任何位置打开设备电源时，设备完整性会自动得到验证，从而建立安全监管链，而无需手动干预。这样，您就可以扩展运营，并确保基础架构从一开始就安全无虞。

NativeEdge 端点经过优化，可与 NativeEdge 兼容，并在戴尔工厂使用加密安全性受到保护。

NativeEdge 利用安全组件验证 (SCV) 流程来确保硬件组件的真实性和完整性。通过 SCV，NativeEdge 可实施供应链完整性、组件验证、固件验证、安全启动流程和加密签名，防止未经授权的访问或篡改。

这些设备经过基于 FIDO 的设备接入流程时，其完整性会自动得到认证，从而确保从戴尔工厂制造到部署站点接收和安装，全程保持安全性。如果硬件受到任何篡改，平台会自动将其隔离，保护运营免受恶意组件的侵害。

接入安全设备并应用零信任框架

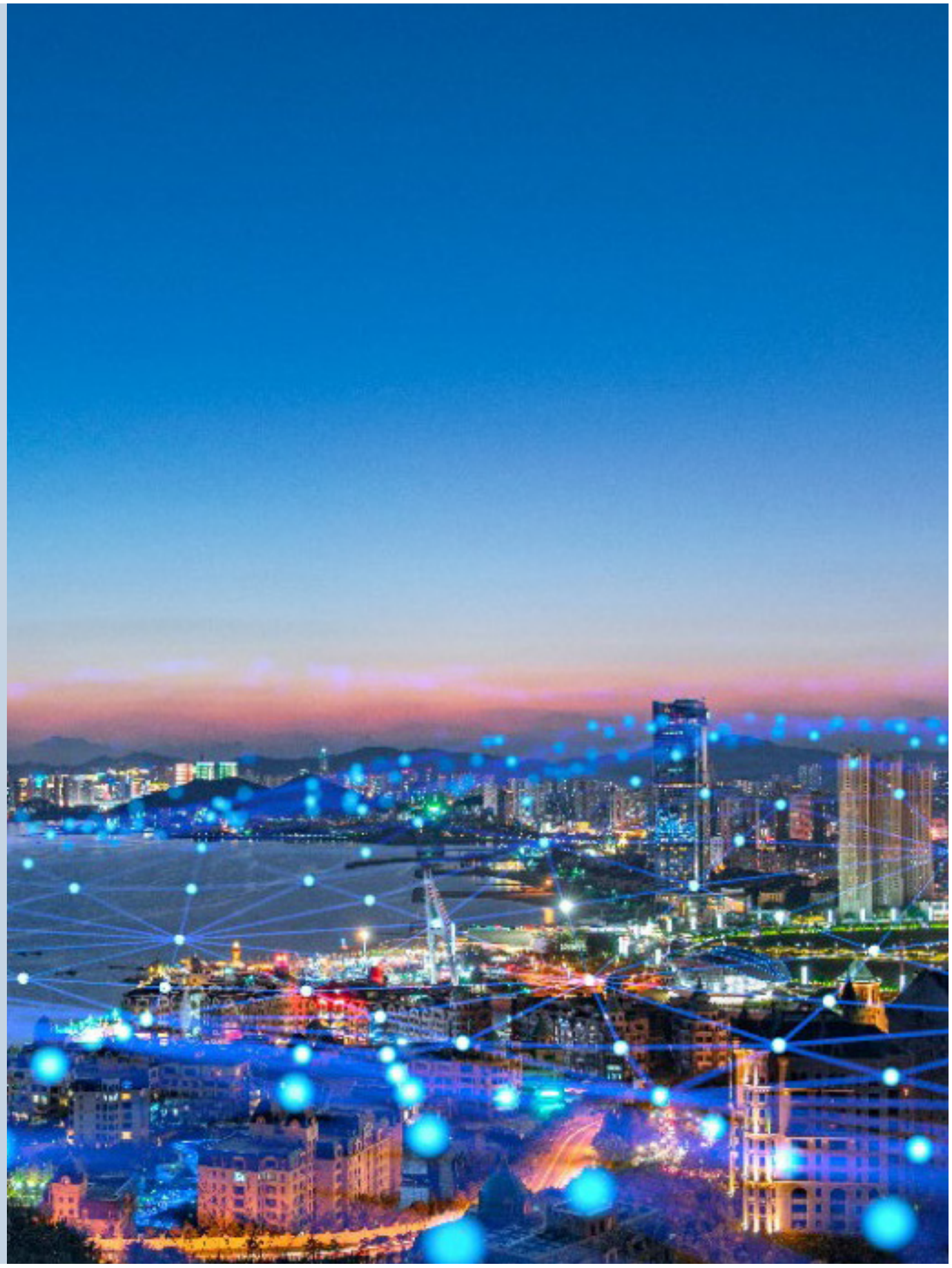


强化从边缘到云的各类数据和应用程序

以一家全球零售商为例。由于零售环境的不同和分布性，访问应用程序和工作负载的用户的身份可能无法经过例行验证。即便实施了验证，也仅限于在环境本地进行，无法集中查看和审计。

此外，零售商通常无法了解已部署应用程序的软件供应链情况。这些应用程序通常由托管服务提供商 (MSP) 处理，他们可能不会对这些应用程序的保真度进行任何可见的自动检查。这些应用程序最初通常由相同的 MSP 进行配置，随着时间的推移，配置可能会发生偏差。因此，利益相关者无法确定应用程序是否符合安全策略。

对于制造商，运营技术 (OT) 团队通常运行一系列不同的应用程序工作负载。其中一些应用程序与 PLC 等设备交互，是不具有内部可见性的专有应用程序。



IT 网络功能不会流向逻辑上分离的 OT 网络，其结果是，制造商 OT 网络内的基础架构和应用程序工作负载无法访问促进安全 OT 环境所需的网络安全控制。各行各业都存在与应用程序和数据安全相关的类似挑战。

Dell NativeEdge 可帮助组织保护从数据源到本地或云中运行的应用程序的数据管道。它结合了加密、用户访问控制、应用程序蓝图目录、网络分段和安全编排等高级安全措施。NativeEdge 还使用遥测和分析来主动评估分布式位置的安全态势，而无需依靠具有审计能力的专家到访每个站点。

高级安全措施

高级安全措施确保运营弹性

用户访问控制

NativeEdge 提供基于角色的访问控制 (RBAC)，可根据用户的角色和职责解析访问权限级别。设备和已部署应用程序工作负载的用户会在每次访问会话中受到验证，并通过身份和访问管理，以集中、可见的方式进行证明。

网络分段

通过对应用程序网络进行微分段，可以更轻松地开发和管理针对这些应用程序的策略，从而提高其安全性。这种方法可降低虚拟化环境中潜在漏洞和威胁横向移动的风险。

应用程序蓝图目录

NativeEdge 旨在提高应用程序的安全性。这基于一个安全的软件供应链，该供应链依赖蓝图目录来部署应用程序。该目录集合了独立软件供应商 (ISV) 提供的应用程序的部署蓝图，或企业开发并经戴尔预先验证的蓝图，所有这些蓝图都旨在维护安全的软件供应链。这些蓝图基于 TOSCA 标准和 YAML 格式，可同时在多个边缘设备上自动部署应用程序和 AI 框架。借助 NativeEdge，您可以在精细级别为已部署的应用程序设置主动式安全控制，并确保您的应用程序得到一致部署并符合您的安全策略。最后，应用程序工作负载可以在 NativeEdge 端点上运行，或作为虚拟机和容器在多云环境中运行，由 NativeEdge 集中管理。

数据加密和保护

无论数据位于何处，无论数据处于静态、传输中还是使用中，NativeEdge 都能妥善保护数据，防止数据被泄露或受到未经授权的访问。NativeEdge 提供强大的静态数据加密 (DARE) 功能，可满足联邦合规性标准，确保您存储的数据得到加密，并防止物理被盗或篡改。NativeEdge 通过零信任安全原则管理每项数据资源，实施严格的访问控制并持续证明和验证访问控制。这不仅可以保护企业应用程序的数据完整性，还可以增强所有业务利益相关者的信心。

安全编排

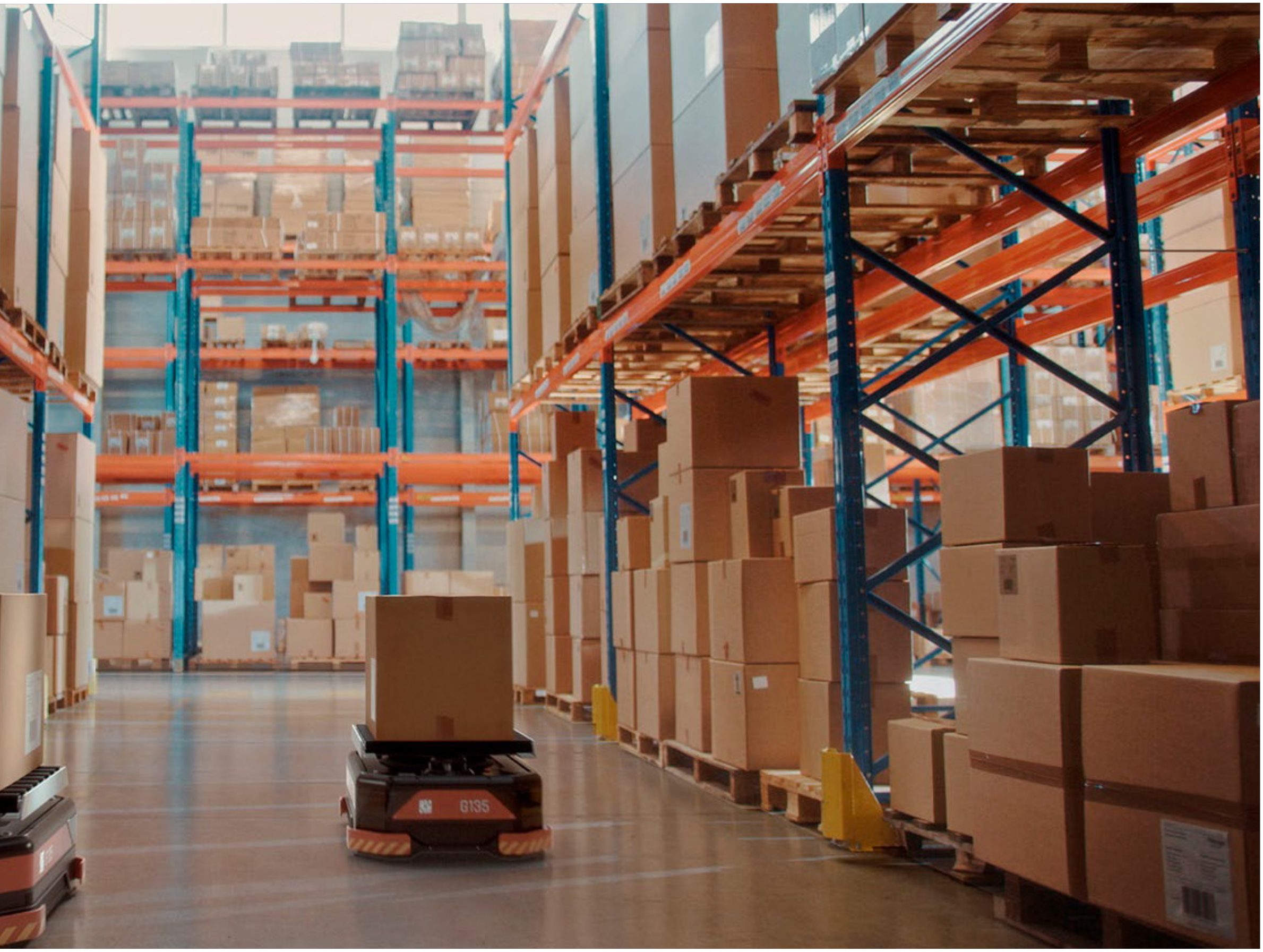
未经授权的操作/事件往往难以察觉，并且通常不会得到补救。这在人工流程下会带来风险，并且常常不及高优先级的业务任务受到重视。此外，IT 集成在身份访问管理 (IAM)/基于角色的访问控制 (RBAC) 和控制平面上存在差异。

这会导致安全编排的割裂，通常需要在每个站点单独管理。在许多 OT 场景中，这些设备处于机器对机器 (M2M) 环境中，完全不具备用户感知能力。集中式编排对于这些环境至关重要。

NativeEdge 可确保跨边缘资产进行一致的安全编排。它基于边缘环境中发生的所有操作和事件，可提供安全态势的统一视图，从而在所有站点实现集中式身份验证和一致的策略实施。它使用 IAM 和 RBAC 功能，允许使用最小特权原则对平台进行安全管理，从而提供企业所需的粒度。NativeEdge 还通过自动执行记录和配置管理，简化对 GDPR、PCI 和 HIPAA 等法规的合规性，帮助您在任何环境中自信地运营，并且能够整合监管、风险与合规性 (GRC)/安全运营 (SecOps) 的规则。

遥测和分析

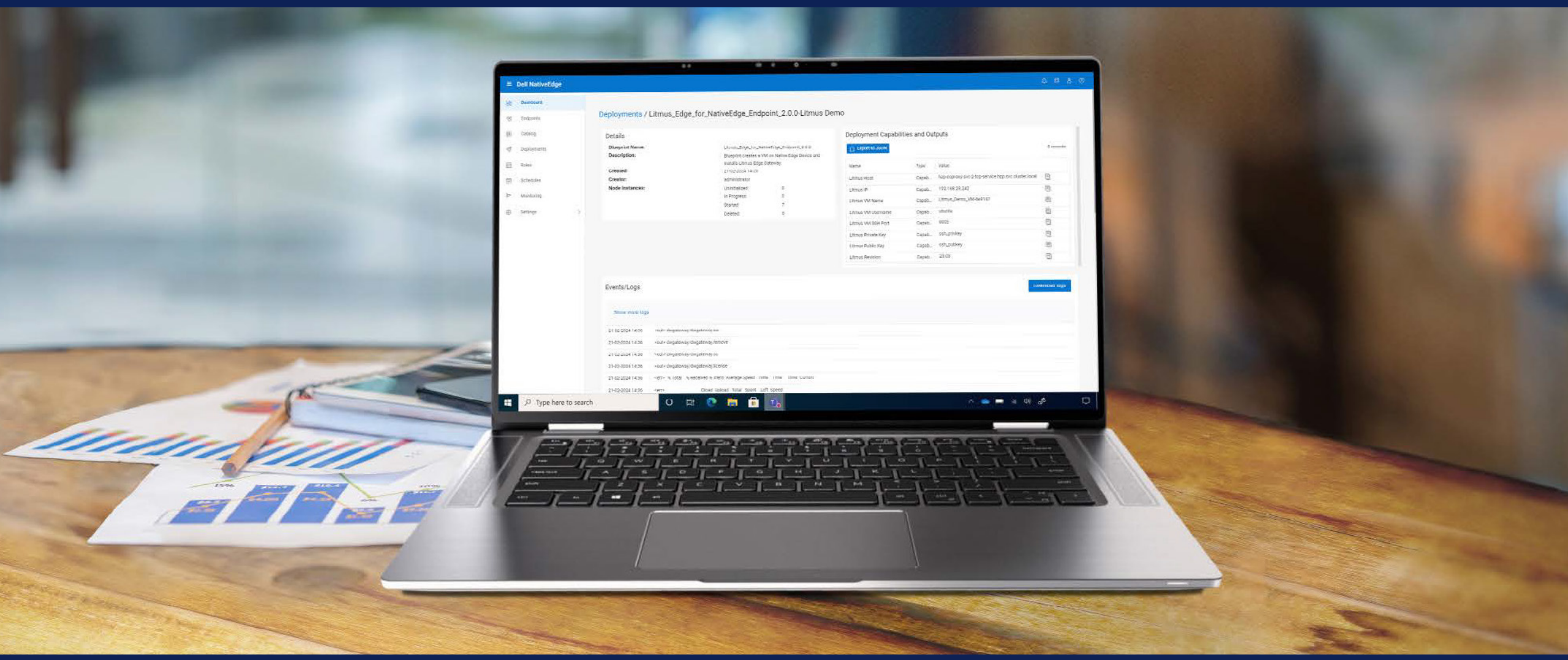
NativeEdge 依靠来自硬件和操作环境的遥测，根据定义的合规性标准持续执行安全评估。这些安全评估用于确定配置偏差检测、配置错误以及是否需要安全更新。



保护边缘资产

Dell NativeEdge 通过零信任安全原则保护您的边缘资产，包括基于 FIDO 的安全设备接入以及经过强化且安全的 NativeEdge OS。借助 Dell NativeEdge，您可以放心地确保您的基础架构、用户、网络、应用程序和数据在分布式位置得到持续证明与验证。

随时随地，锐意创新



DELL Technologies

有关详情，请访问 **Dell.com/NativeEdge**