Dell NativeEdge

Protect: Operate confidently with zero-trust security

Table of

Contents

Security throughout distributed environments

To meet rapidly changing customer preferences and market dynamics, organizations are deploying new applications, updates, and compute infrastructure at an unmatched volume and velocity. This deluge of data, infrastructure, and applications means it is becoming increasingly critical to secure the distributed environments where these new technologies reside.

As enterprises expand operations, they become increasingly vulnerable to security risks – ranging from physical device tampering to data hacking. Additionally, these systems often handle sensitive personal data, placing more responsibility on enterprises to protect their customers.

To secure operations, enterprises need to

Ensure
the physical safety of the infrastructure deployed in distributed locations

Detect
device tampering and remediate threats

Control
user access at every level

Scale
provisioning and software updates across thousands of devices

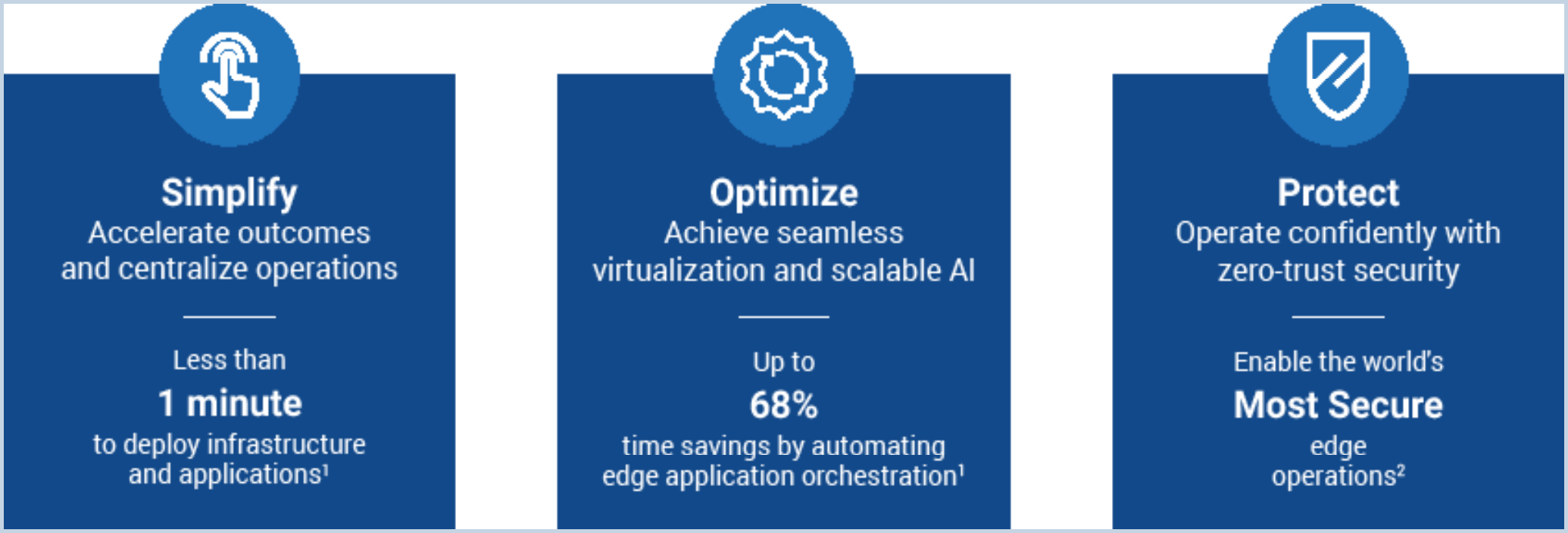
Dell NativeEdge

Innovate wherever you operate

A full-stack, end-to-end solution that securely centralizes the deployment, orchestration, and lifecycle management of diverse infrastructure and applications at the edge and across distributed data centers.

Simplify, optimize, and protect edge and distributed data center environments with features such as zero-touch onboarding, zerotrust security, and advanced workload orchestration. NativeEdge leverages a KVM hypervisor and container run-time allowing organizations to deploy and manage both virtual machines (VMs) and containers. It is optimized to orchestrate AI workloads and frameworks, enabling seamless deployment and management of AI-driven applications at the edge and throughout distributed data centers. NativeEdge can also adapt to any hardware environment, supporting a wide range of options in various form factors, from Dell PowerEdge servers to desktops as well as third-party infrastructure.

Dell NativeEdge is purpose-built to address the unique challenges of distributed environments, such as operational complexity, scalability, and security. It's a solution tailored for modern organizations focused on harnessing the power of edge computing while reducing costs and improving efficiency.



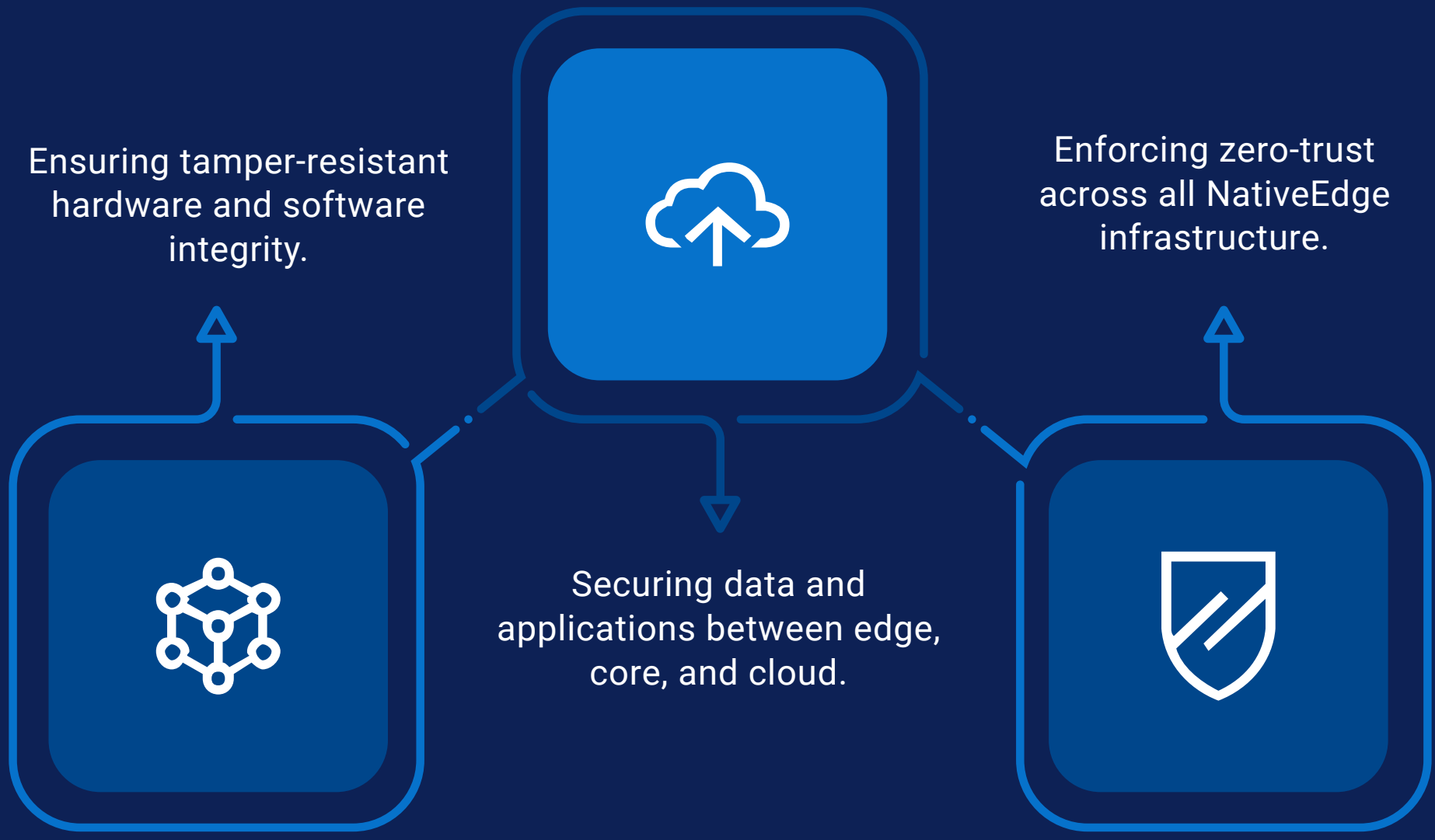
[1] Enterprise Strategy Group by TechTarget Technical Validation commissioned by Dell Technologies, "Dell NativeEdge Edge Operations Software Platform,"February 2025.

[2] Based on Dell Technologies Internal analysis, May 2025.

Dell.com/NativeEdge

Secure your expanding distributed operations by persistently and automatically reinforcing security of infrastructure, applications, data, network, and users without any IT intervention.

Dell NativeEdge protects distributed operations by



Reinforcing zero-trust security

Modern enterprises are responsible for managing thousands of applications throughout geo-distributed sites and often rely on a heterogeneous mix of infrastructure. This creates a complex web of technology silos that are inefficient to manage, difficult to secure, and slow to update. As organizations continue to deploy new applications, new sensors, and new devices to distributed locations, the attack surface for potential cyber-threats grows.

How can enterprises ensure the ongoing security of distributed data operations?

Dell NativeEdge empowers you to operate with confidence with a foundation of zero-trust security. From the moment a device is powered on, a hardware-rooted chain of trust is established, utilizing features like UEFI Secure Boot and a virtual Trusted Platform Module (vTPM) to ensure device integrity. Built in support for GDPR and other global data sovereignty mandates, NativeEdge offers peace of mind for distributed environments. This approach, combined with capabilities like zero-trust micro-segmentation, safeguards your applications and data so you can innovate securely wherever you operate.

Zero-trust security

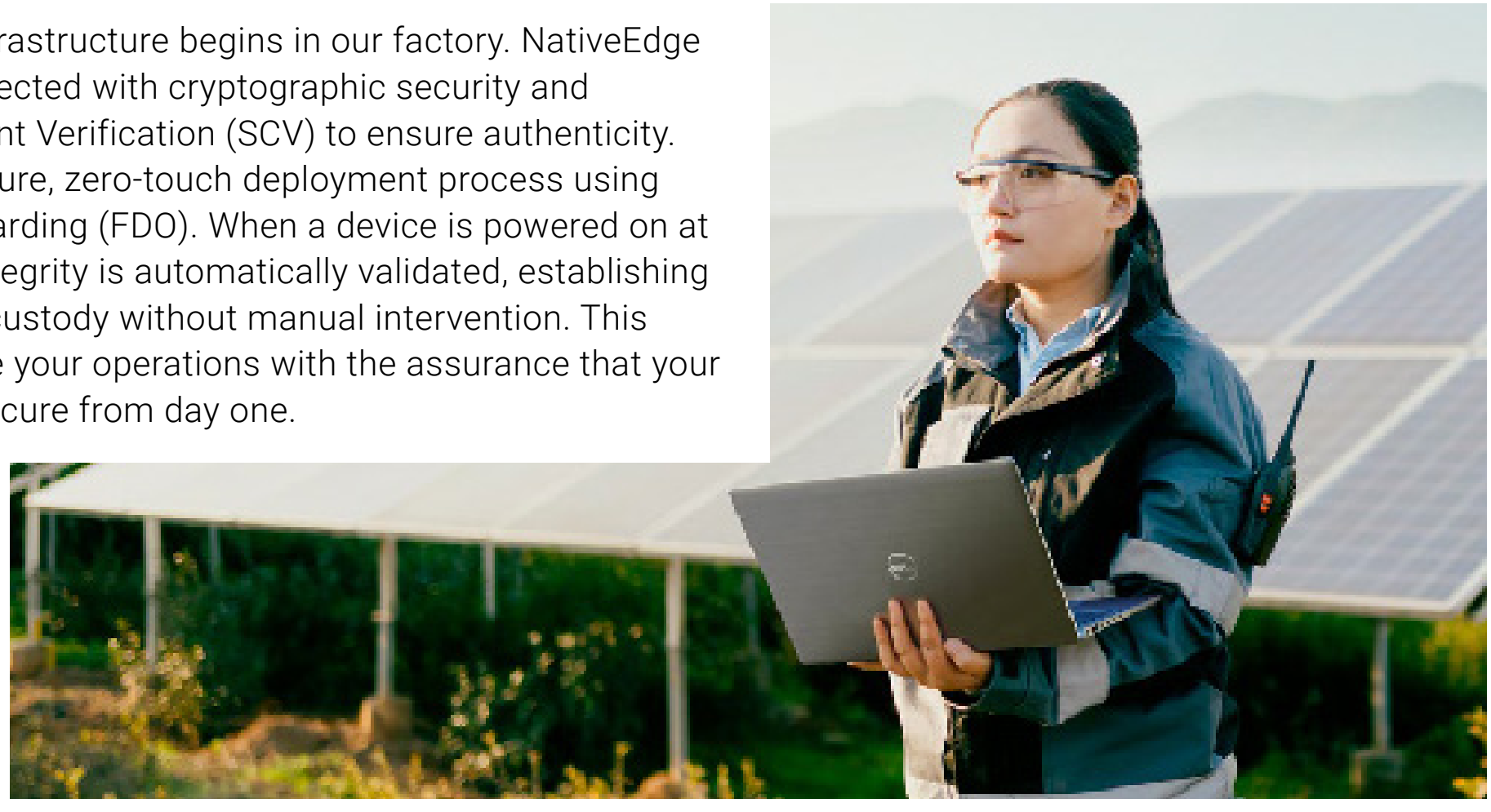
The security posture is further strengthened by monitoring and understanding all actions of your resources, enabled by relevant business controls, a centralized control plane, and an infrastructure that is explicitly working on its behalf. With the zero-trust design principles of NativeEdge, enterprises can rest assured that as distributed operations expand, the integrity of every connected resource is continuously attested and validated.

Ensuring hardware integrity through the supply chain and its lifecycle

Looking at the examples of a retailer or manufacturer with global store or factory locations, it becomes increasingly difficult to manage and secure the diverse hardware that has varying specifications and profiles based on location. Over time, these devices aren't continuously attested, and the compliance can't be verified on an extended time scale. This risk grows exponentially when multiple parties are included in the installments of these devices.

How can you consistently protect distributed infrastructure?

Protecting your infrastructure begins in our factory. NativeEdge Endpoints are protected with cryptographic security and Secured Component Verification (SCV) to ensure authenticity. This enables a secure, zero-touch deployment process using FIDO Device Onboarding (FDO). When a device is powered on at any location, its integrity is automatically validated, establishing a secure chain of custody without manual intervention. This allows you to scale your operations with the assurance that your infrastructure is secure from day one.

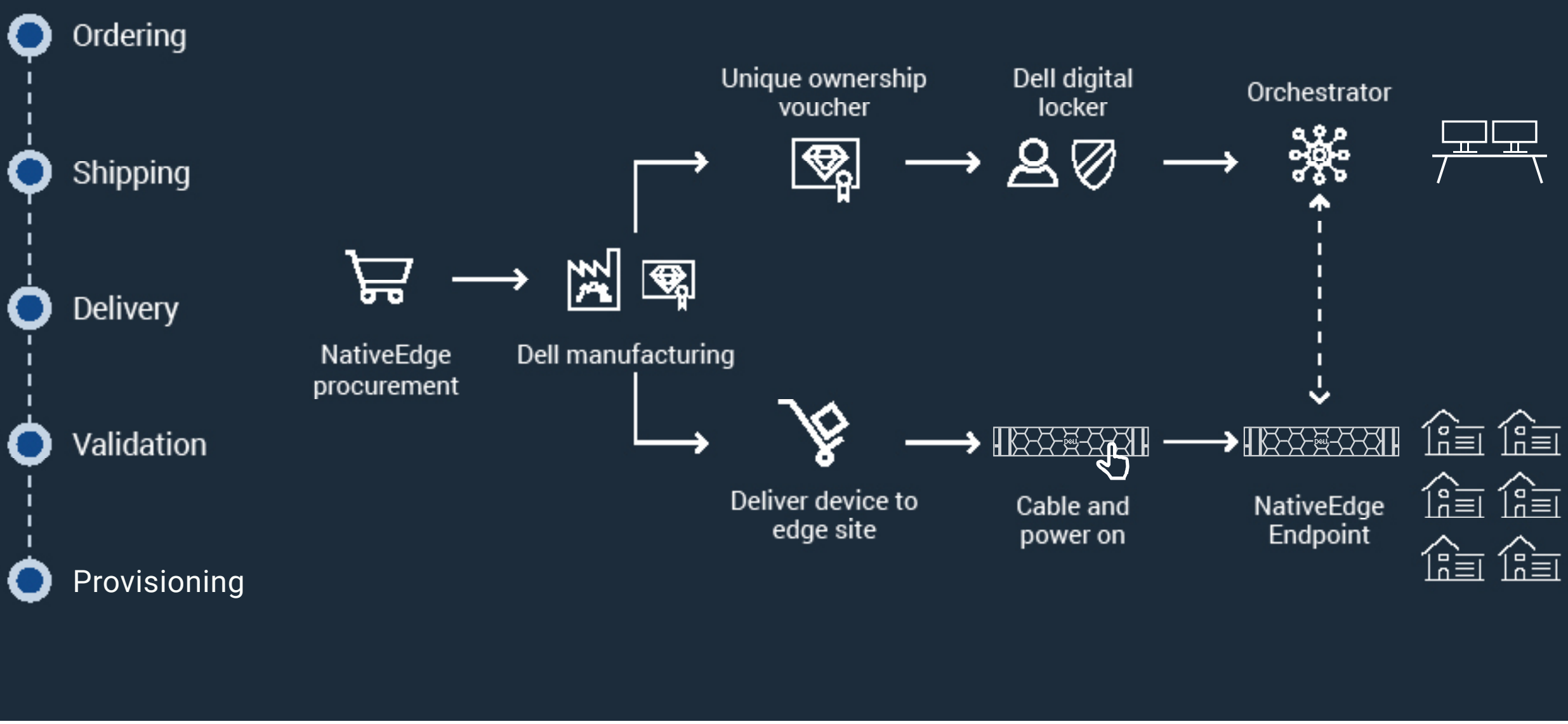


NativeEdge Endpoints are optimized for compatibility with NativeEdge and protected with cryptographic security at the Dell factory.

NativeEdge leverages the Secured Component Verification (SCV) process to ensure the authenticity and integrity of hardware components. Through SCV, NativeEdge enforces supply chain integrity, component verification, firmware validation, secure boot processes and cryptographic signatures to protect against unauthorized access or tampering.

As these devices go through the FIDO-based device onboarding process, their integrity is certified automatically, ensuring security from manufacturing in the Dell factory all the way to receipt and installation at the deployment site. If hardware is tampered with in any way, the platform automatically isolates them, protecting operations from rogue elements.

Secure device onboarding and a zero-trust framework

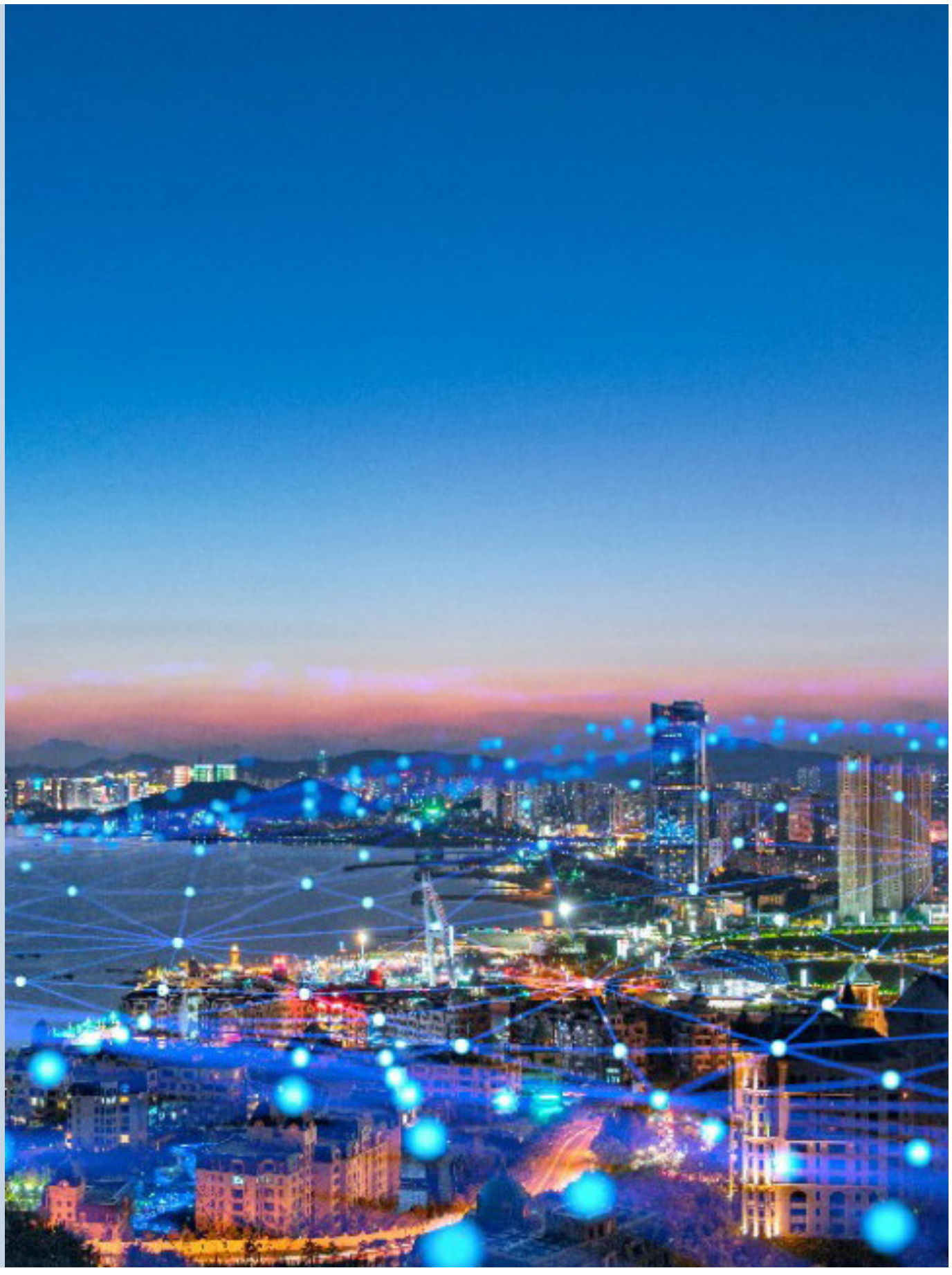


Fortifying data and applications from edge to cloud

Consider the example of a global retailer. The disparate and distributed nature of retail environments means the identities of users accessing applications and workloads might not be routinely verified. If they do, it is local to that environment and not centrally visible and auditable.

Furthermore, retailers seldom have visibility to the software supply chain of deployed applications. These are often handled by Managed Service Providers (MSPs) and there may not be any visible automated checks of the fidelity of these apps. These applications are often initially configured by the same MSPs, with the possibility of configuration drifting as time goes on. Therefore, stakeholders are unable to determine application compliance with security policies.

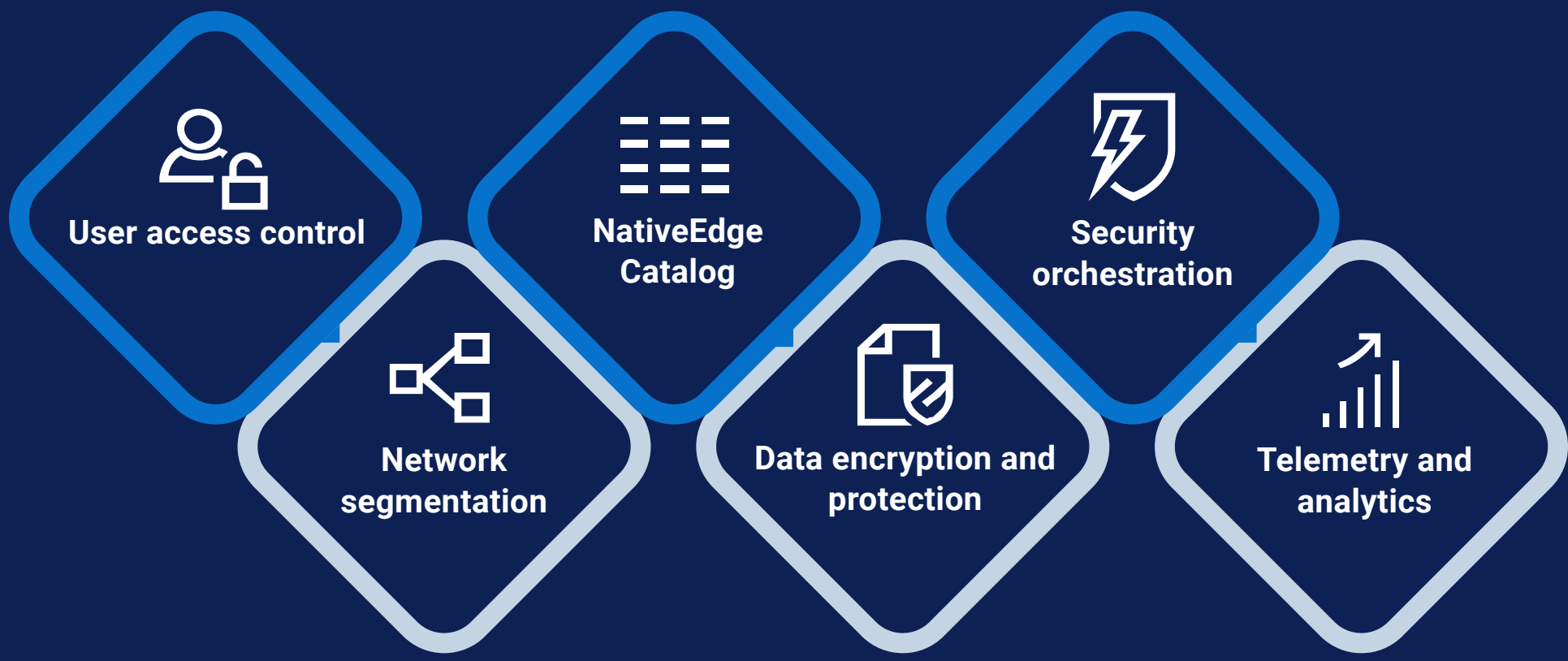
In the case of manufacturers, the operations technology (OT) team generally runs a diverse set of application workloads. Some of these applications interface with equipment such as PLCs and are proprietary applications without internal visibility.



IT network capabilities do not flow down to the OT network, which is logically separate The result? infrastructure and application workloads inside the manufacturers' OT networks do not have access to the level of network security controls that are needed to facilitate a safe OT environment. Similar challenges related to application and data security are common across all industries.

Dell NativeEdge helps organizations secure the data pipeline from data sources to the applications running locally or in the cloud. It combines advanced security measures such as encryption, user access control, application blueprint catalog, network segmentation, and security orchestration. NativeEdge also uses telemetry and analytics to proactively assess the security posture of your distributed locations without relying on experts with audit capabilities to visit every site.

Advanced security measures



Advanced security measures ensure resilient operations

User access control

NativeEdge provides role-based access control (RBAC) to parse levels of access based on an user's roles and responsibilities. Users of the devices and deployed application workloads are verified per access session as well as attested in a centralized and visible fashion through identity and access management.

Network segmentation

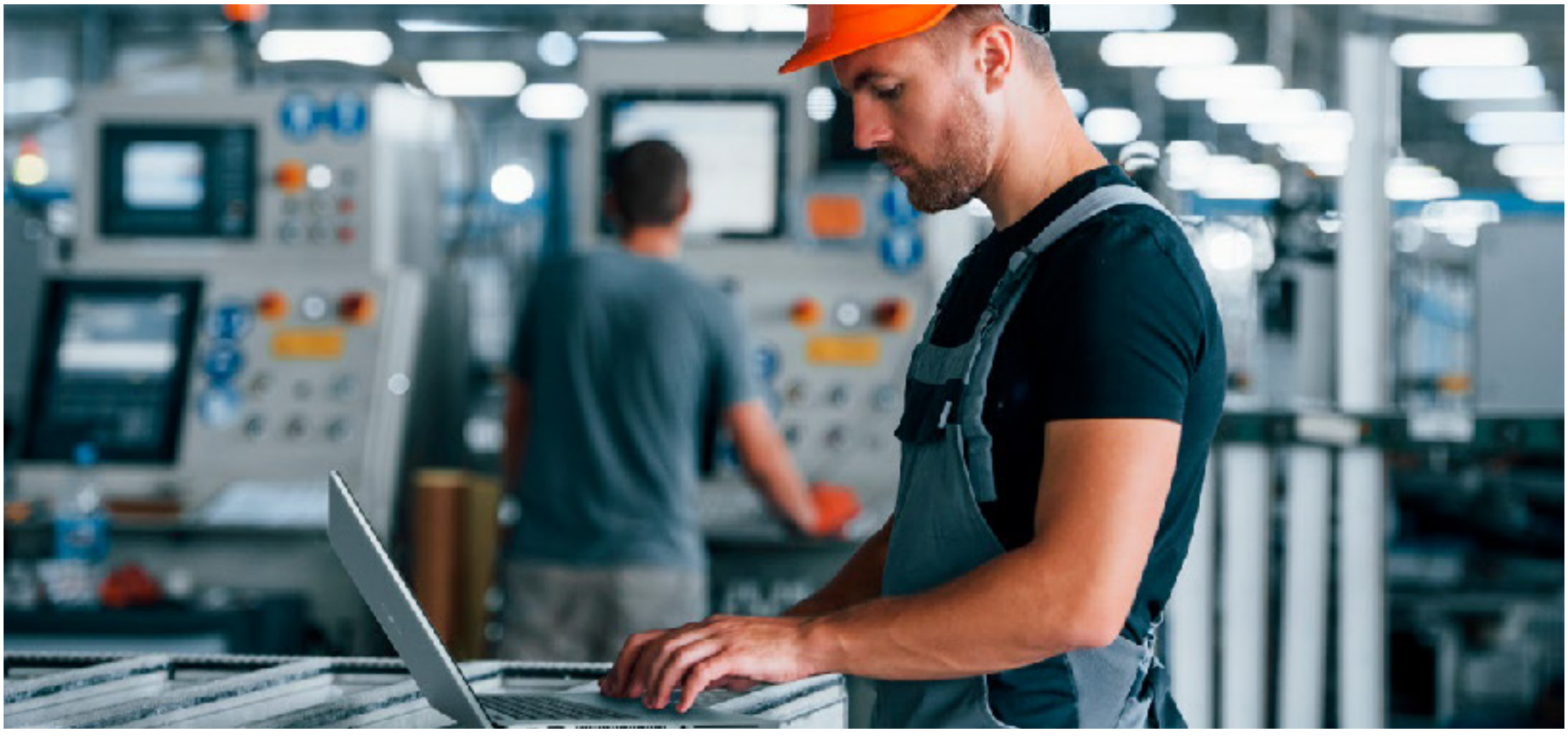
Micro-segmenting the network for the applications makes it easier to develop and manage policies that target these applications to make them more secure. This approach mitigates the risks of potential breaches and the lateral movement of threats within virtualized environments.

Application Blueprint Catalog

NativeEdge is designed to make applications more secure. It starts with a secure software supply chain that relies on a Catalog to deploy your applications using blueprints. The Catalog is a collection of blueprints to deploy applications from Independent Software Vendors (ISVs) or pre-validated blueprints from Dell developed by enterprises, all to maintain a secure software supply chain. These blueprints, based on the TOSCA standard and YAML format, automate the deployment of applications as well as AI frameworks across many edge devices at once. NativeEdge allows you to set proactive security controls for deployed applications at a granular level and ensures your applications are deployed consistently and aligned with your security policies. Finally, the application workloads can run on NativeEdge Endpoints or in a multicloud environment as VMs and containers, managed centrally by NativeEdge.

Data encryption and protection

NativeEdge protects your data wherever it resides—at rest, in transit, and in use - against breaches and unauthorized access. NativeEdge provides robust data at rest encryption (DARE), which meets federal compliance standards, ensuring your stored data is encrypted and protected against physical theft or tampering. NativeEdge governs every data resource with zero-trust security principles, enforcing strict access control and continuously attesting and verifying the access control. This not only protects the data integrity for enterprise applications but also boosts the confidence of all business stakeholders.



Security orchestration

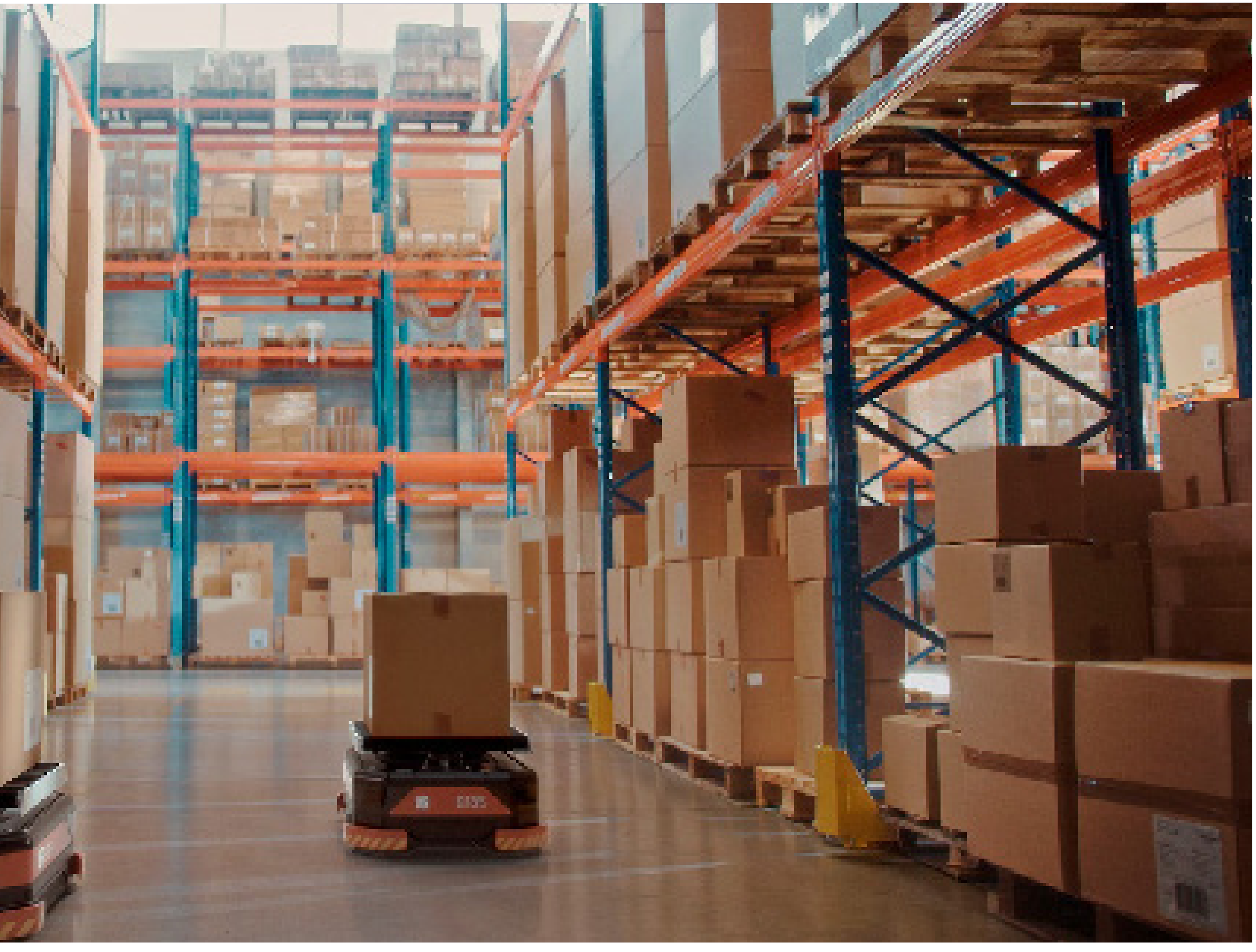
Unauthorized actions/events often occur unnoticed and often are never remedied. This introduces risk due to manual processes and often takes a back seat to high-priority business tasks. In addition, there exists variation across IT integration around Identity Access Management (IAM)/ Role-Based Access Control (RBAC), and control plane.

This leads to a disconnected security orchestration which is often managed individually at each site. In many OT cases, these devices are in a Machine-to-Machine (M2M) environment which has no user awareness. Centralized orchestration is crucial for these environments.

NativeEdge ensures consistent security orchestration across the edge estate. Based on the aggregate of actions and events that happen in the edge environment, it provides a unified view of your security posture, enabling centralized authentication and consistent policy enforcement across all sites. It uses IAM and RBAC capabilities that allow secured management of the platform using the principle of least privilege, thus providing the granularity that enterprises need. NativeEdge also simplifies compliance with regulations like GDPR, PCI, and HIPAA by automating logging and configuration management, helping you operate confidently in any environment with the ability to incorporate rules from Governance, Risk, and Compliance (GRC)/ Security operations (SecOps).

Telemetry and analytics

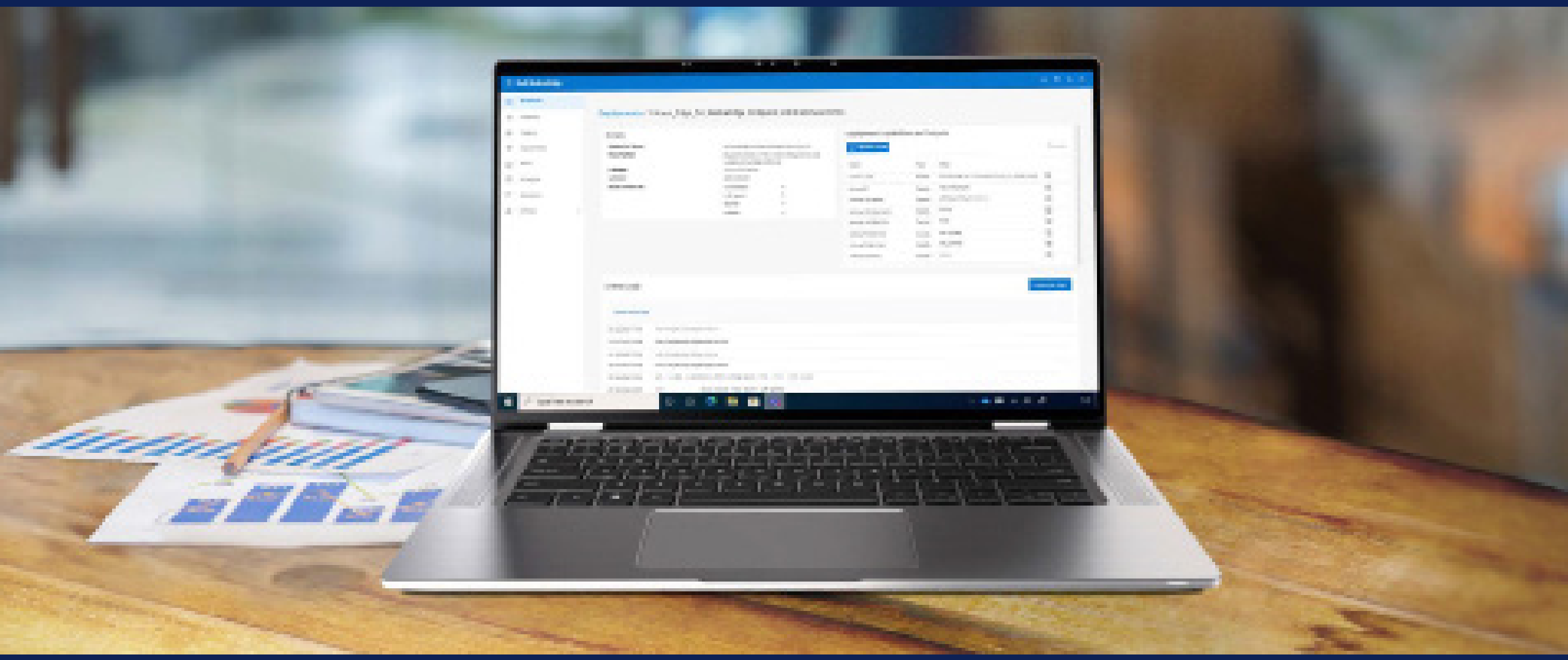
NativeEdge continuously performs security assessments in line with defined compliance standards by relying on telemetry from the hardware and operating environment. These are used to determine configuration drift detection, misconfiguration, and the need for security updates.



Protect your edge estate

Dell NativeEdge protects your edge estate with zero-trust security principles including FIDO-based secure device onboarding coupled with a hardened and secure NativeEdge OS. With Dell NativeEdge, you can rest assured that your infrastructure, users, network, applications, and data are continuously attested and validated across distributed locations.

Innovate wherever you operate



DELL Technologies

Learn more about **Dell.com/NativeEdge**