

Introduction to the Dell NativeEdge Software Platform

August 2023

H19628

White Paper

Abstract

This white paper introduces the Dell NativeEdge operation software platform. The paper describes the value proposition and architecture of the software platform.

Dell Technologies Solutions

Copyright

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Intel, the Intel logo, the Intel Inside logo and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Other trademarks may be trademarks of their respective owners. Published in the USA 08/23 White Paper H19628.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Executive summary4

Business challenge.....6

About NativeEdge7

NativeEdge Orchestrator8

NativeEdge-enabled Devices11

Applications.....14

Conclusion.....16

References16

Executive summary

Overview

Dell NativeEdge is an edge operations software platform that offers fleet management and application orchestration to the edge, core data centers, and cloud. With NativeEdge, customers can simplify edge operations, optimize edge investments, and secure the edge.

Audience

This document is intended for IT administrators, Operations Technicians (OT), solution architects, partners, Dell Technologies employees, and individuals who may evaluate, acquire, manage, operate, or design an edge environment using NativeEdge.

Terminology

The following table provides definitions for some of the terms that are used in this document.

Table 1. Terminology

Term	Definition
Application Catalog	Collection of applications provided by ISVs, home-grown, third party, along with the necessary configurations and application metadata.
Deployments	Applications from the catalog are deployed as VMs and running on NativeEdge-enabled Devices.
Edge Devices	A list of all the NativeEdge-enabled Devices and their VMs.
FIDO Device Onboard (FDO)	Main technology used to provide Secure Device Onboarding with FDO. Reference FIDO Device Onboard Specification 1.1 for more information.
NativeEdge-enabled Device	Select Dell edge hardware optimized for the platform with the NativeEdge Operating Environment for secure device onboarding and to provide a secure and scalable operating environment to run edge applications as VMs.
NativeEdge Orchestrator	Management component built into the edge platform that provides hierarchical security, orchestration, and life cycle management of vertical solutions distributed across the edge, core, and edge local deployments.
NativeEdge Operating Environment	A combination of a Linux-based operating system, KVM hypervisor, and an orchestrator agent that enable the devices to work with the NativeEdge platform.
Onboarding Service	This service supports the FIDO Device Onboard protocols to bind the NativeEdge-enabled device to the NativeEdge Orchestrator and allow the orchestrator to provision the device.
Rendezvous Service	A networking service that runs inside the NativeEdge Orchestrator that determines how the newly powered-on NativeEdge-enabled Devices connect to the NativeEdge Orchestrator.
Secure Device Onboard with FDO	The process of securely adding one or many NativeEdge-enabled Devices to the Edge estate.

**We value your
feedback**

Dell Technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell Technologies Solutions team by [email](#).

Author: Jonathan Tang

Contributor: Rana Moussa

Note: For links to additional documentation for this topic, see [Dell Technologies Info Hub for Edge Solutions](#).

Business challenge

Recent years have seen a significant shift towards the edge, as more companies deploy devices that have a demand for more data and analytics. By deploying devices to the edge, companies can reduce latency, improve the speed of data processing, and enhance security. Also, deploying devices at the edge can also help reduce bandwidth consumption and minimize the costs that are associated with transmitting large amounts of data to the cloud. The deployment of devices to the edge has therefore become a crucial component of modern technology infrastructure, enabling businesses to improve their operational efficiency and deliver better customer experiences.



Figure 1. Challenges at the edge

However, unique challenges require a new approach to the edge. The diversity of hardware and environments makes testing, integrating, deploying, and managing hardware and associated software a critical design point. Edge application workloads are challenging because they must support diverse use cases like computer vision in manufacturing or inventory management in retail. Large-scale geo-distributed locations such as retail stores and distribution centers elevate business-level concerns surrounding security, support, and efficient distributed systems operations. The installation of these systems must prioritize simplicity and must be zero-touch once plugged in and powered on. Secure operations require the ability to bring edge devices into your environment with zero-trust security in mind. Having multiple solutions for specific use cases can lead to technology silos that become operationally challenging.

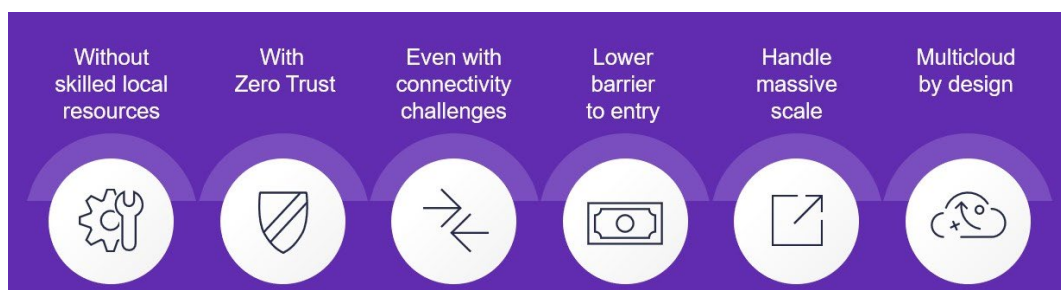


Figure 2. New approach to edge operations

The NativeEdge solution tackles these challenges by reimagining the approach to edge operations. The solution offers a way to overcome challenges without relying on local

skilled resources. Users only need to plug in and power on the device. The rest of the process is fully automated. NativeEdge also ensures security, leveraging secure device onboarding and zero trust security from the point of manufacture, throughout the supply chain, to the point of production and through the retirement of the device. NativeEdge supports a wide range of protocols and networking configurations. It also accommodates unpredictable network services or isolated designs. NativeEdge has the flexibility to start small, which enables commence operations on a small scale, with a single device, and expand in any direction within the same location or across multiple sites. Moreover, it is designed for multicloud workloads that can be centrally monitored and managed, allowing for the deployment of applications from the edge, core, and any cloud of choice.

About NativeEdge

The NativeEdge operations software platform enables organizations to securely deploy and manage infrastructure at the edge. NativeEdge can support a wide range of NativeEdge-enabled Devices and uses zero trust principles, factory integration, and application orchestration to create a secure edge environment. It can start small with a single device and scale out as needed and can be centrally deployed globally regardless of network connectivity, technology staffing, or specific environment.

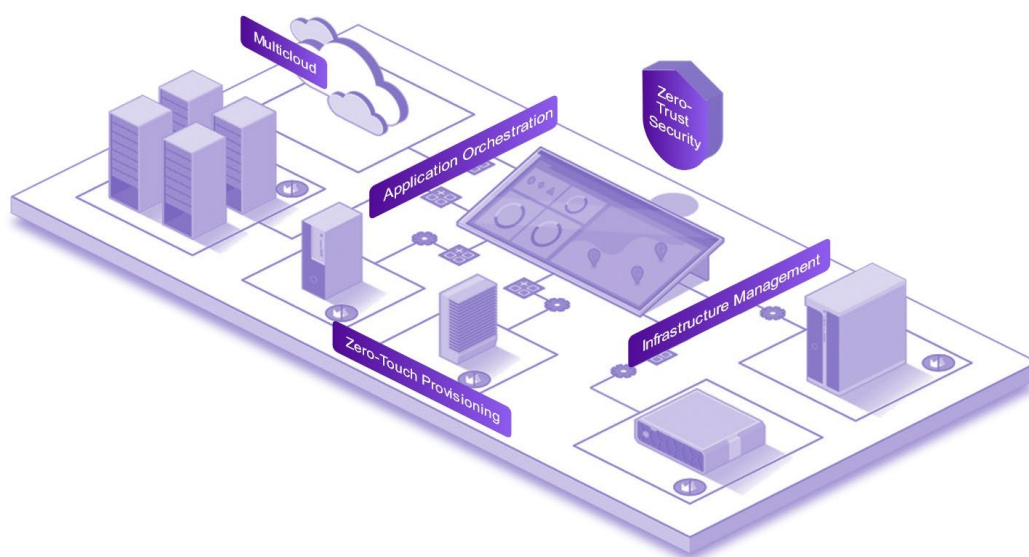


Figure 3. NativeEdge operations software platform

NativeEdge Orchestrator

At the center of NativeEdge is the orchestrator, which supports edge operations such as application orchestration, fleet management, and life cycle management. Packaged as Helm charts, the NativeEdge Orchestrator can be deployed anywhere a dedicated Kubernetes cluster exists. For example, the Kubernetes cluster can be on-premises inside a VM or bare-metal server. Once the NativeEdge Orchestrator is deployed, customers can easily add NativeEdge-enabled Devices into the edge estate with secure device onboarding and zero-touch provisioning. For more information about how to install the NativeEdge Orchestrator, see the Dell NativeEdge Orchestrator Deployment Guide on the Support Site.

Secure device onboarding with FIDO

Traditionally, the installation of edge devices has been a laborious and time-consuming process. It often involved individuals like retail store managers or factory plant managers, who might lack the expertise to manage complex edge devices and operating system installations. This highlights the importance of ensuring that edge devices are user-friendly and straightforward to deploy.

To address this need, Dell introduces NativeEdge, a solution that simplifies the deployment of NativeEdge-enabled devices while ensuring robust security with zero trust and zero-touch capabilities. With NativeEdge, anyone can set up a NativeEdge-enabled device by plugging in a network cable, powering on the device, and stepping away. Dell is partnering with Intel along with the FIDO (Fast Identity Online) Alliance to make this streamlined installation process easy. From this collaboration, Dell is leveraging the open standard managed by the Alliance, known as FIDO FDO (Device Onboarding) specification 1.1.

During the manufacturing process, a digital record known as an ownership voucher is created for every NativeEdge-enabled device. This voucher is a public key based off a hash that is stored within the TPM (Trusted Platform Module) of the device. Once NativeEdge-enabled devices have been ordered and built, customers can access their ownership vouchers through Dell Digital Locker. For example, if a customer orders 50 NativeEdge-enabled Gateway 3200s, there are 50 ownership vouchers stored with the customer's Dell Digital Locker account. Keeping a copy of these ownership vouchers allows a customer to validate the NativeEdge-enabled Device as it travels through the supply chain.

After successfully deploying the NativeEdge Orchestrator, customers are presented with two options for uploading vouchers, as shown in the figure below. The first method referred to as "Non-Air-Gapped," involves establishing an Internet connection between the NativeEdge Orchestrator and Dell Digital Locker. Through a one-time security exchange, vouchers are automatically downloaded from Dell Digital Locker and integrated into the NativeEdge Orchestrator.

Alternatively, for environments with firewalls or physical network separations that prevent direct access to Dell Digital Locker, customers can opt for the "Air-Gapped" method. In this approach, customers manually download the vouchers to their local laptop or workstation and then upload them to the NativeEdge Orchestrator once they are within the confines of their secure network.

Upload Voucher ✕

This page will allow you to upload your device vouchers. Once the upload completes, power on your device to onboard them.

What type of connectivity do you have?

☒ Non Air-Gapped (connected to the internet) ☐ Air-Gapped (not connected to the internet)

Follow these steps to get your NativeEdge Orchestrator token:

- Click [here](#) to log in the Dell Digital Locker, and follow the steps when prompted to get the NativeEdge Orchestrator token.
- Copy the NativeEdge Orchestrator token from the Dell Digital Locker, and paste it below.

[Cancel](#) Upload

Figure 4. Upload Vouchers

After uploading vouchers into the NativeEdge Orchestrator, they are automatically registered with a rendezvous service that runs inside the NativeEdge Orchestrator. When this step is completed, the TO0 (Transfer Ownership 0) has been completed as part of the FDO specification 1.1. For a list of vouchers within the NativeEdge Orchestrator UI, navigate to **Settings > Entitlements** as shown in the following figure.

Dell NativeEdge

Entitlement

[Vouchers](#) [Tokens](#) [License](#) [Certificates](#)

This page allows you to upload vouchers.

NativeEdge Orchestrator Identifier: [Copy to Clipboard](#)

Upload 5 vouchers

Service Tag	GUID	Upload Date
4N960G3	75986515-020d-48cd-bc08-ca6b79a51f97	06-Jul-2023 02:20:53 PM
1XHTFT3	2c26ab4e-0e66-4f0f-bfe4-a91e22e9e344	06-Jul-2023 04:08:02 PM
CXCK6X3	5d99c802-76b1-4d29-92ec-e90c5b13c5a9	13-Jul-2023 09:43:21 AM
DXCK6X3	9c2c1a22-b963-40ce-acbd-01c560a2c9f6	19-Jul-2023 11:23:18 AM
7XHTFT3	300e8a43-dc0b-4268-83df-6bdee2e417a3	20-Jul-2023 03:27:01 PM

Show: 25 per page 1 of 1

Figure 5. Voucher Entitlement page

When a customer receives the NativeEdge-enabled device and powers it on, it automatically starts looking for the rendezvous service. It will attempt to cycle through a set of preprogrammed addresses “rv.local.edge”, “rv1.local.edge”... “rv20.local.edge” until

it finds the voucher that matches the NativeEdge-enabled Device. The rendezvous service will then return information about the onboarding service within the NativeEdge Orchestrator. When this step is completed, the TO1 (Transfer Ownership) has been completed as part of the FDO specification 1.1. If there is no voucher match, the device automatically attempts a reonboard after some time. Customers will need to preconfigure their DNS servers and point these FQDN addresses to the IP address of their NativeEdge Orchestrator. If customers do not have a DHCP or DNS server, they can use the service console loaded on a local VM or workstation to set the IP address and rendezvous service manually. For more information about how to configure DNS mapping, see the Dell NativeEdge Orchestrator Support Site.

The final step of the onboarding process is connecting to the onboarding service. This step involves establishing secure communication between the NativeEdge-enabled Device and the NativeEdge Orchestrator over port 443. During this step, mTLS credentials are established and stored within the TPM of the device. This is the final step known as TO2 (Transfer Ownership 2) as part of the FDO specification 1.1. From this point, the NativeEdge-enabled Device automatically downloads, installs, and reboots into the NativeEdge Operating Environment. Users have the flexibility of loading different versions of the NativeEdge Operating Environment by setting different profiles for the different families of devices (PowerEdge, OptiPlex, and Dell Edge Gateways).

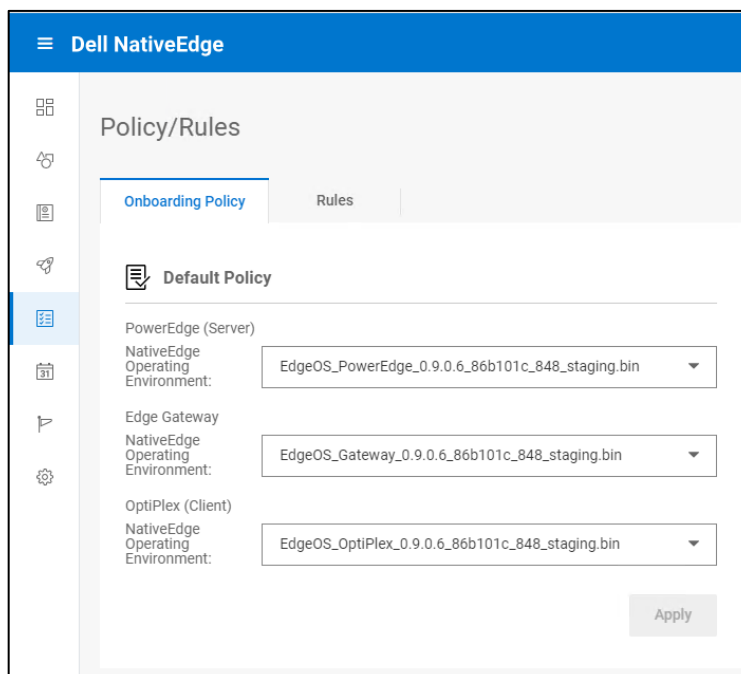


Figure 6. NativeEdge Operating Environment Profiles

Fleet management

The NativeEdge Orchestrator is a comprehensive solution that enables fleet management for customers of all sizes. By leveraging a centralized platform, customers can begin with a limited number of edge devices and effortlessly expand alongside their business growth. After adding NativeEdge-enabled Devices into the NativeEdge Orchestrator, administrators can perform a wide range of tasks such as inventory management, monitoring of alarms and events, servicing and troubleshooting edge devices, and life cycle management such as NativeEdge Operating Environment upgrades or firmware

updating the edge devices. For more information about how to manage the NativeEdge-enabled Devices, reference the Dell NativeEdge Orchestrator User's Guide on Info hub.

NativeEdge-enabled Devices

NativeEdge offers a wide range of supported models, with form factors ranging from Dell Edge Gateways, OptiPlex towers, and PowerEdge servers. For the full list of supported edge devices, see the following table. After the user powers on the device at their site, the Dell NativeEdge operating system is automatically installed on each endpoint device. This operating system acts as a Linux-based KVM hypervisor, enabling support for VM-based applications deployment. The NativeEdge-enabled Devices also have a secure and encrypted communication channel to the NativeEdge Orchestrator using SSL or TLS protocols over HTTPS.

NativeEdge also offers comprehensive support for hardware upgrades such as adding additional network cards, additional storage devices, memory, CPU, and other components. These upgrades are limited to products sourced from Dell and approved for compatibility.

Table 2. Supported Dell NativeEdge-enabled Devices

Dell Edge Gateway	OptiPlex	PowerEdge
EGW-3200 EGW-5200	XE4 Small Form Factor	R660 R760 XR4510c XR4520c

Secure boot

At the edge, there are security risks where devices are typically deployed in remote and less secure locations, making them vulnerable to physical tampering of devices. Furthermore, when these devices are shipped throughout the supply chain, the device could be exposed to of multiple different parties where there could be a malicious actor somewhere throughout the supply chain. That is why every shipment of NativeEdge-enabled Device from the Dell manufacturing plant is secure and locked down. This is accomplished by the following:

- Secure Boot enabled in BIOS – Only Dell NativeEdge images such as Factory OS, NativeEdge Operating Environment, factory reset image, and so on will boot successfully.
- BIOS password protected and lockout
- Boot order lockdown
- Secure Component Validation (for PowerEdge R660 and R760)
- iDRAC (for PowerEdge models) is disabled during onboarding
- Single network port available during onboarding

Factory OS

The Factory OS is a lightweight operating system installed onto the NativeEdge-enabled Device during the manufacturing process. This OS serves as a staging operating system and is not intended to be the final OS used by the end user. The Factory OS is immutable,

meaning it remains unchanged and cannot be written to or modified in any manner. In simpler terms, each boot-up of the Factory OS is identical.

Also, the Factory OS is designed with a high level of security and is locked down, providing no console access. In case of troubleshooting, users can use a **Service Console** that is loaded onto a laptop or workstation and can set IPs, DNS addresses, and collect logs. For more information about how to use the Service Console, see the Dell NativeEdge User's Guide on the Support site.

The Factory OS runs the following services upon boot-up:

- Service Console Listener
- Secure Component Validation (PowerEdge R660, and R760 only)
- FIDO Device Onboard Client
- Automated download and installation of the NativeEdge Operating Environment.

NativeEdge Operating Environment

The NativeEdge Operating Environment is the final operating system that is automatically installed onto the NativeEdge-enabled Device after onboarding is complete. It is based on an open-sourced Linux operating system that supports virtual machines for customer-edge applications. Like the Factory OS, this operating system is also fully immutable. With this operating system, all network ports are enabled including iDRAC for PowerEdge models, however, the service console is now disabled.

Datastores

Datastores are a logical construct within NativeEdge that allows customers to store their applications once they have been deployed onto a NativeEdge-enabled Device. Datastores are encrypted either using hardware-based encryption if Self-Encrypting Drives (SEDs) are available. Otherwise, software encryption will be leveraged if there are no SEDs available. Datastores are automatically created by the NativeEdge Operating Environment giving the best performance and high availability to protect customer applications in case of a disk loss. If there is no storage controller for RAID, the system automatically create datastores based on a few factors such as the protocol of the drive (NVMe or SCSI), speed of the drive (for example 7200 RPM or 5400 RPM), and size (for example 2 TB or 1 TB). Datastores can be viewed in the **Hardware > Storage** tab on the device detail page as shown below.

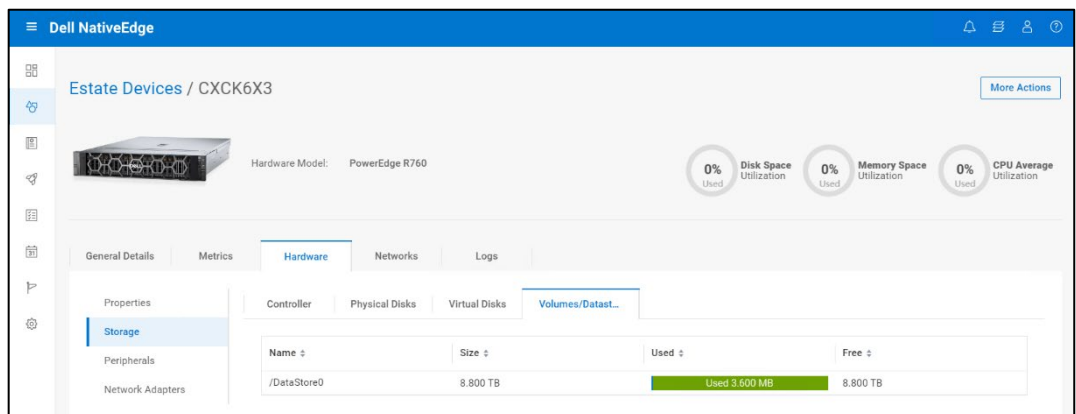


Figure 7. Datastores

Networks

NativeEdge supports two different types of networks. Host networks and virtual network segments. Host networks are used for management networks for the NativeEdge-enabled Device to communicate to the NativeEdge Orchestrator. Users can create, modify, and delete host networks, but they cannot delete the default network that is automatically created by the system. The host network can also be used by customer application VMs if they deploy applications with the NAT virtual network segment type and port forwarding enabled.

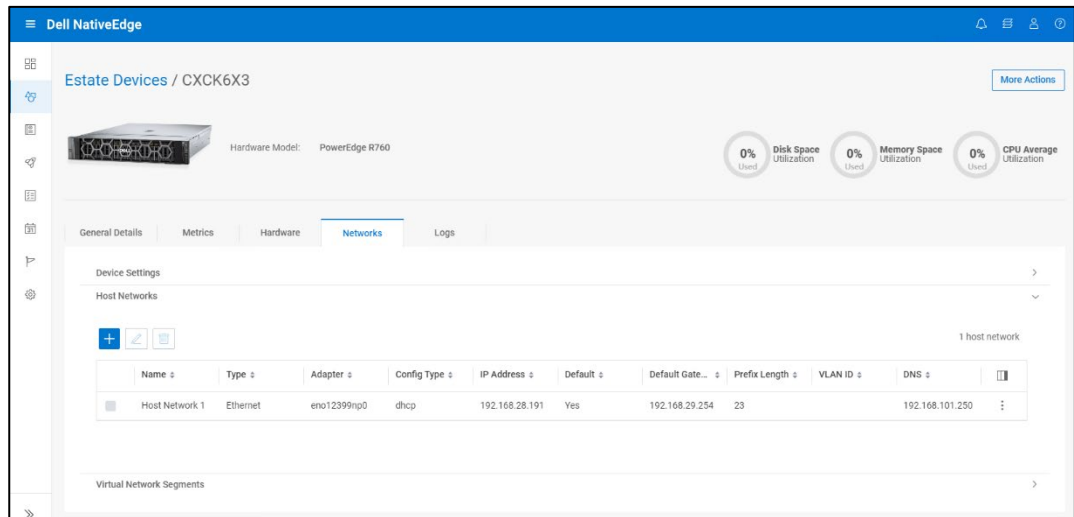


Figure 8. Host Networks

Customers can also create virtual network segments for customer applications. NativeEdge supports the creation of multiple virtual network segments on top of a single Ethernet port. There are three different types of virtual network segment types:

- NAT (Network Address Translation)
- Air-gapped
- Bridged

NAT virtual network segments have their own DHCP, DNS, and IP Address management scheme. By default, they do not have any visibility outside this network unless source NAT and port forwarding rules are created. In this scenario, VMs would have network connectivity to devices outside of the virtual network segment and would use the host network for connectivity.

Air-gapped virtual network segments are like NAT VNS. It provides its own DHCP, DNS, and IP management scheme, however, it does not have any external network connectivity. This scenario is useful for test-dev purposes where there could be two VMs that need to perform tests.

Bridged virtual network segments are networks that are visible to a customer's existing network environment. For example, if a customer has an existing DHCP and DNS server that a VM needs access to, this would be a good example to assign the VM to a bridged network. Bridged networks also support VLANs in access and trunk mode configuration.

Applications

Application Catalog

Deploying applications at the edge can be challenging for OT personnel such as retail store managers, or factory plant managers because they may not have the skill set to configure complex application solutions. In addition, these users may not know about life cycles manage and patch applications that may be vulnerable to security risks. With NativeEdge, customers can centrally manage application images, set up virtual networking and life cycle manage the application if security patches are needed.

The orchestrator offers an Application Catalog that enables customers to centrally manage applications for their entire edge environment. An application could be a virtual machine that runs on top of the NativeEdge-enabled Device after the installation of the NativeEdge Operating Environment. NativeEdge supports many image formats including raw, ISO, qcow2, VDI, VHD, and VMDK. Customers can upload applications i two different ways. The first method known as “Local” supports uploading images up to 50 GB in size from an image stored on a local workstation. If customers have images larger than 50 GB, they can upload images from an “External” repository that is from a remote file stored on an HTTP repository.

The screenshot shows a web-based form titled "Add Application". On the left is a sidebar with three tabs: "Application Information" (active), "Configuration", and "Summary". The main content area is under the "Application Information" tab and includes the following fields and options:

- Application Information**: This page allows you to enter file information for the application being added.
- Specific Information**:
 - Type: VM
 - Name: Test-Application
 - Description (Optional): [Empty text box]
 - Version: 1.0
 - Developer: Dell
 - Icon: Dell_Logo.svg.png [BROWSE button]
 - License (Optional): [Empty text box]
- Files** (The Section allows you to add the application files that will be uploaded):
 - Repository: ☒ Local ☐ External
 - Filename: custom-application.qcow2 [BROWSE button]
 - Description (Optional): [Empty text box]

At the bottom right of the form are "Cancel" and "Next" buttons.

Figure 9. Add Application

When applications are being added, users can set certain compute constraints based on CPU, memory, and storage requirements based on the application needs. Setting these limits allows users to have a filtered list of eligible NativeEdge-enabled Devices to be shown at the time of deployment. Users also can set virtual network interfaces and selecting passthrough devices such as serial, USB, GPU, and video. In some situations, there may be some customized configuration that may be needed during the first bootup of applications. NativeEdge offers the capability of passing custom parameters such as strings, numerics, or passwords as optional keys or value pairs that are available to the virtual machine upon first boot. These variables can then be used by scripts and utilities running inside the virtual machine to perform customization. For example, an application may accept a STORE_LOCATION environment variable to set up configuration for a specific store.

After an application is uploaded, there may be situations where new versions of the applications need to be uploaded due to new features or patches. The Application Catalog supports adding newer versions by selecting the **More Actions > Add Using Existing** option when selecting an existing application. Users will need to supply a new version and new image. Once the new version is uploaded, the **application catalog** will display a different version for application deployment. If users have existing applications that are deployed and would like to upgrade them, they can navigate to the **Deployments** page and highlight the application they would like to update, and then **select More Actions > Update Deployment**.

Name	Version	Description	Type	Minimum ...	Minimum ...	Minimum ...	Deployments
CAC Demo	2.0		VM	2	2.0 GB	10.0 GB	0
Demo123	1.0		VM	2	2.0 GB	10.0 GB	1
Demo1234	1.0		VM	2	2.0 GB	10.0 GB	2
Focal	1.0		VM	2	2.0 GB	10.0 GB	0
Focal	1.5		VM	2	2.0 GB	10.0 GB	1
Focal VM	1.0	VMDK	VM	2	2.0 GB	10.0 GB	1
Test App	1.0		VM	2	2.0 GB	10.0 GB	2
Ubuntu - ISO	22.04		VM	2	2.0 GB	10.0 GB	0

Figure 10. Updating Application

Deploying applications

To deploy applications, users have the flexibility of choosing between two methods: manual deployment or deployment through user-defined rules. In the manual deployment process, users start on the **Application Catalog** page, selecting the application, and then click the **Deploy** button. A wizard presents a list of filtered NativeEdge-enabled Devices on the resource constraints that were set up during the initial upload of the application. Users can select a 1:1 deployment or 1: many deployments.

For example, if an administrator wanted to deploy a point-of-sale application to 50 different sites, they could select all 50 different NativeEdge-enabled Devices for the NativeEdge Orchestrator to automatically install. After the NativeEdge-enabled Devices are selected, users can select the datastore for where the applications are stored, and the network settings and any port forwarding if required.

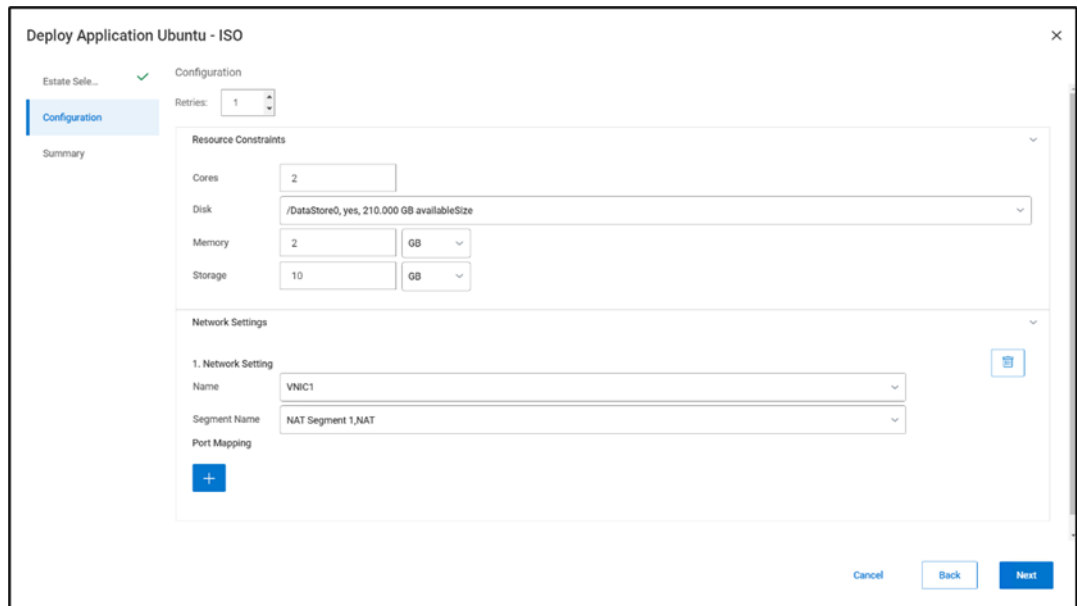


Figure 11. Datastores and Networks

Another method of deploying applications revolves around user-defined rules that use resource tags for automating the deployment process. Resource tags can be applied to both NativeEdge-enabled Devices and applications, enabling logical grouping of objects. For instance, users can create resource tags based on location for 50 OptiPlex devices in the US and then establish a rule to automatically deploy applications based on these resource tags. For detailed instructions on how to set up resource tags and rules, refer to the Dell NativeEdge User's Guide on Info hub.

Conclusion

Dell NativeEdge helps customers simplify their edge operations. It enables data processing and analytics closer to the source, reduces latency, and minimizes the need for data to be processed in the cloud. Using NativeEdge, customers can simplify their edge operations with secure device onboarding and zero-touch provisioning. Also, the NativeEdge software platform offers a set of features and supported by a robust ecosystem that is required to address the challenges of the modern era.

References

The following [Dell Technologies documentation](#) provides additional relevant information.

- Dell NativeEdge Orchestrator User's Guide
- Dell NativeEdge Security Configuration Guide
- Edge Security Essentials: Edge Security and How Dell NativeEdge Can Help
- Dell NativeEdge DevOps Brief