Solution Brief

Resilient Edge Virtualization with NodeWeaver

Introduction

At the edge, it can be challenging to maintain legacy workloads, develop/deploy new applications, and create a scalable technology stack that allows stakeholders to efficiently manage manufacturing technology. One way organizations look to solve this challenge is by endeavoring to virtualize both new and legacy applications. While there are a vast array of virtualization tools available, not all are suited for edge deployments. While it may be tempting to use virtualization tools that your IT organization has standardized on for data center and cloud, not considering the unique complexity of the edge can lead to operational inefficiencies, downtime, and stunted growth of digital transformation initiatives.

The evolving convergence of IT and OT (Operational Technology) is an essential element in creating infrastructure that is both highly resilient to application downtime and maintains a high standard of security to prevent unauthorized access to critical business data. Many of the skills to manage virtualized infrastructure have historically been developed by IT professionals, further underscoring the point that these groups need to work together when it comes to edge virtualization.

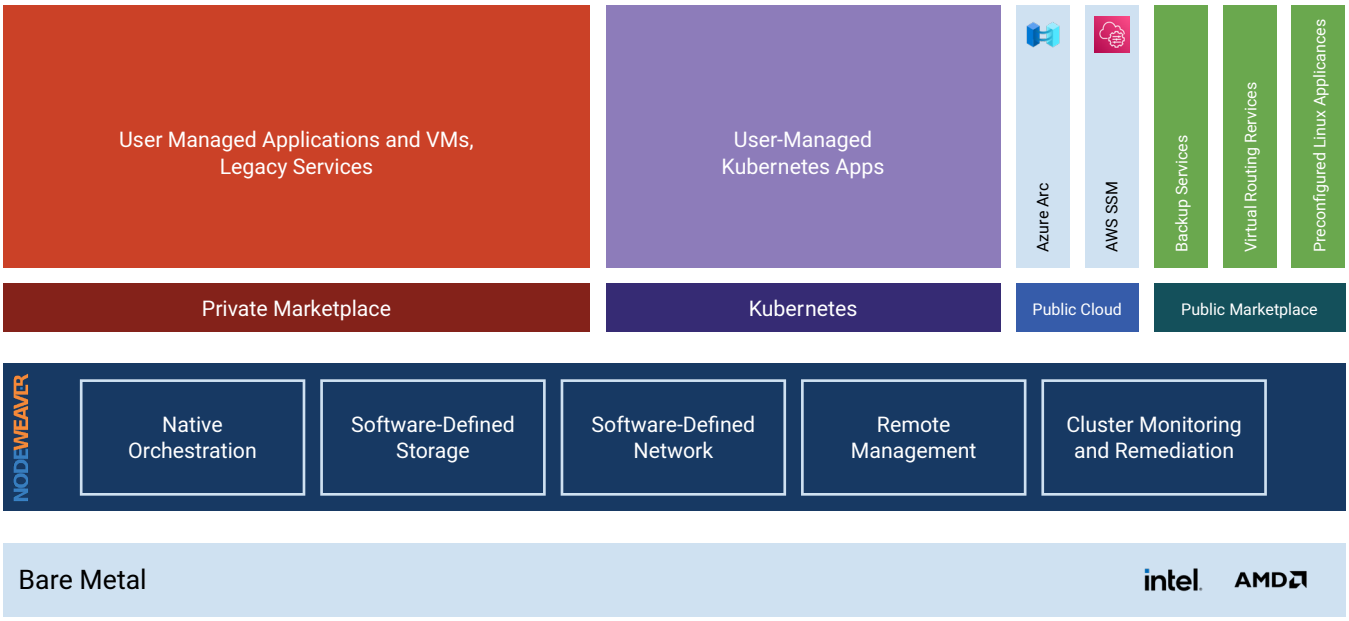
What is NodeWeaver?

OnLogic has partnered with NodeWeaver to empower users with a highly-reliable edge virtualization solution. NodeWeaver is a zero-management Edge cloud fabric - integrating storage, networking and virtualization in a single system. It has an easy to use interface and a management system that automates most tasks and helps simplify activities that would otherwise require highly skilled expensive personnel.

NodeWeaver delivers linear and predictable edge deployment scale-out without large up-front investments. Having a unified compute, storage and networking platform enables organizations to deploy the applications required without complex planning and procedures. NodeWeaver's Distributed File System aggregates internal and direct-attached storage resources across all nodes, presenting it as a single storage entity and making it available to all hosts.

Solving Virtualization Challenges at the Edge

To bring virtualization to the edge a platform needs to overcome typical challenges for edge workloads, create resilience to downtime, and secure the network against threat actors.



- **Deploying and Managing Distributed Infrastructure**
  - Deploying and managing devices spread across hundreds of sites is challenging. Users need the ability to centrally manage all nodes while enabling disconnected operations. For fleet-level management NodeWeaver offers their patented DNSOps and EdgeInsight tools to monitor and manage all devices centrally at scale. While the autonomy engine deployed on each cluster manages each cluster's workloads automatically.

- **Limited Computing Horsepower**
  - Many virtualization platforms have high compute overhead to manage complex features and tools. While this can be fine in the datacenter, at the edge there's often a need to scale down platforms to lower power devices running 1-2 VMs. NodeWeaver only consumes 1 Core and 1GB of RAM, which makes it ideal for edge deployments ranging from small quad-core gateways to large Intel Xeon or AMD Epyc-based edge servers.
- **Building Edge Applications for Scale**
  - A common challenge many users face is balancing hardware spend with the future goals of the organization. For example, imagine a cluster of systems running virtualized applications as part of a Distributed Control System (DCS) and sensor collection platform at an oil & gas refinery. The business is happy with the results and wants to expand to processing video streams from thermal cameras for pipeline monitoring. However, existing systems do not have the capacity to support the GPUs needed for inference. With NodeWeaver, hardware can be heterogeneous, allowing different hardware solutions to be added and managed as part of an existing cluster.
- **The Cost of Expertise**
  - Edge computing solutions should not require special skills or tools to implement. When certified technicians are required to implement virtualization, this can easily increase CapEx by 3-4x the initial cost of the hardware. Additionally, if resources are limited, waiting on a 3rd-party technician to come on-site increases average downtime and adds to ongoing maintenance costs. For platforms that support zero-touch deployments, such as NodeWeaver, systems can easily be deployed without the need for on-site expertise, allowing organizations to focus on infrastructure investments and application development.

Resilient Edge Virtualization

What if a mission-critical application fails? According to Industry research by Emerson, Industrial Manufacturers lose at least $50 Billion dollars per year due to unplanned downtime.[1] While Siemens estimates downtime costs the automotive industry $2 Million per Hour.[2]

$50 Billion

Annual losses from unexpected downtime, according to Industry research by Emerson.[1]

$2 Million

Hourly cost of downtime for auto OEMs, according to Siemens.[2]

Virtualization that is highly resilient to failure is key to a successful deployment at the edge. How resilient virtualization is built can be defined by two key tenants.

- **Prevention:** Building systems in a manner that will reduce the risk of downtime of applications.
- **Reaction:** Allowing systems to adapt to outside changes to ensure that downtime is avoided or minimized.

Prevention

The first way to address downtime is to prevent it from happening in the first place. Elements of a downtime resistant deployment include:

- **High Availability (HA):** With clustered computing, deploying highly available solutions, i.e. applications that operate even in the event of a hardware or software failure, on the edge increases resilience. Most other platforms require at least 3 nodes as part of a cluster, but with NodeWeaver, HA clusters can be created with just 2 nodes. The ability to achieve HA with fewer nodes can mean the difference between success and failure based on return on investment.
- **Reliable Hardware:** To mitigate the risk of hardware failure its imperative to select reliable edge computing hardware. At the edge, systems can be exposed to wide-temperatures, shock, vibration, and airborne contaminants, which are likely to cause desktop PCs and commercial servers to fail. Total cost of ownership for hardware is important as replacement systems increase project cost by both the cost of hardware and the cost of downtime.
- **Fault Prediction:** While selecting the right hardware goes a long way to reducing failure, nothing can ever be guaranteed. When NodeWeaver is deployed on hardware, it creates a profile of the hardware and the sensors attached to components. This allows for the creation of a model that can provide warnings if it believes a component is beginning to fail, allowing for workloads to start migrating and replicating.

Reaction

Prevention can only take us so far. Systems must also be able to adapt to avoid prolonged downtime. Elements of a successful edge deployment that can help react to downtime events include:

- **Persistent Storage:** Edge applications rely on data ingestion from edge assets, while stateless microservices rely on database connections, any interruption to the ingestion can lead to lost data. OT data is key to mission-critical applications, and data loss can't be tolerated. Persistent shared storage allows applications to retain data even in the event of service failure.
- **Event-Driven Optimization:** Workloads are not static in their resource demands, systems need to react to event-streams dynamically. Platforms must be able to recognize changes and balance resources based on application priority. For critical systems, CPU/RAM/Storage overhead should be considered, so that applications that are load-balanced across a cluster have room for migration in the event of a hardware fault.
- **Intelligent Networking:** The backbone of any edge deployment is networking. In a resilient cluster, networks should be software defined, which allows the cluster to react dynamically to outside events, rerouting traffic as needed. Virtual networking will allow for integration directly with existing IT systems ensuring additional monitoring capabilities and cross-collaboration between working groups.

Secure Edge Virtualization

In addition to preventing downtime and reacting to the unexpected, another key tenant of resilient virtualization infrastructure is security.

According to a 2024 KnowBe4 study,

Cyber attacks on critical infrastructure have increased by 30% since 2022

420 Million per year

8 Million per week

13 Attacks per second [3]

Whether ransomware gangs are looking to extort businesses by holding data hostage, or nation-state actors are attempting to disrupt vital infrastructure and manufacturing, the threat of intrusions into industrial networks has never been higher. While no single best practice, technology or platform will secure a business, virtualization can be part of a comprehensive security framework. Allowing organizations to stay one step ahead of the bad guys, preventing both network downtime and theft of proprietary information.

Air-Gapped Networks

Historically, many organizations have relied on airgapping industrial networks to protect industrial processes. However, many businesses overestimate the security airgapped systems offer.

- Organizations that do not have a wider security plan for OT networks leave themselves exposed to physical exploits at any endpoint on the network, for example via USB device intrusion as seen with GoldenJackal's Malware toolkit targeting embassies in Europe.
- As organizations look to develop edge applications they will want to integrate these systems into existing infrastructure and send OT data to cloud data lakes. It is imperative that additional security controls be implemented to prevent unwanted intrusion, such as DMZ servers and 1-way data diodes.

Platform Security

When looking at edge virtualization platforms, a few key features that NodeWeaver offers include:

- **Cluster Pre-Configuration:** When implementing air-gapped networks as part of a security strategy, clusters can be pre-configured so that additional configuration is not needed. This means systems can be deployed immediately without relying on technicians coming on-site.
- **Workload Isolation:** VMs are isolated and granted the minimum amount of privileges to operate correctly. This should also include encryption of communications, disk encryption, and securing virtualized network connections (such as VXLAN).

- **Boot Security:** Measured Boot and Secure Boot ensure "root of trust" so that only validated software runs on device.
- **Signed Updates:** Ensure that software updates are valid and do not contain malicious/unauthorized code.
- **SASE for Hybrid-Cloud Deployments:** SASE (Secure Access Service Edge) is a framework encompassing a number of technologies, integrated into NodeWeaver, for secure operations between the cloud and edge endpoints. This breaks down to six components:
    - **Software-Defined Wide Area Network (SD-WAN)** → Secure application routing
    - **Secure Web Gateway** → Securing Traffic between Intranets and the Internet
    - **Cloud Access Security Broker** → Monitoring and enforcing cloud security policies
    - **Firewall as a Service** → Ensuring firewalls are integrated into each system with the correct configuration.
    - **Zero Trust Network Access** → Grant the least privileges possible to users when remote access to internal applications is needed.
    - **Central Management** → Manage all systems centrally, automate tasks/updates to ensure all systems stay up to date, and monitor deployed systems.

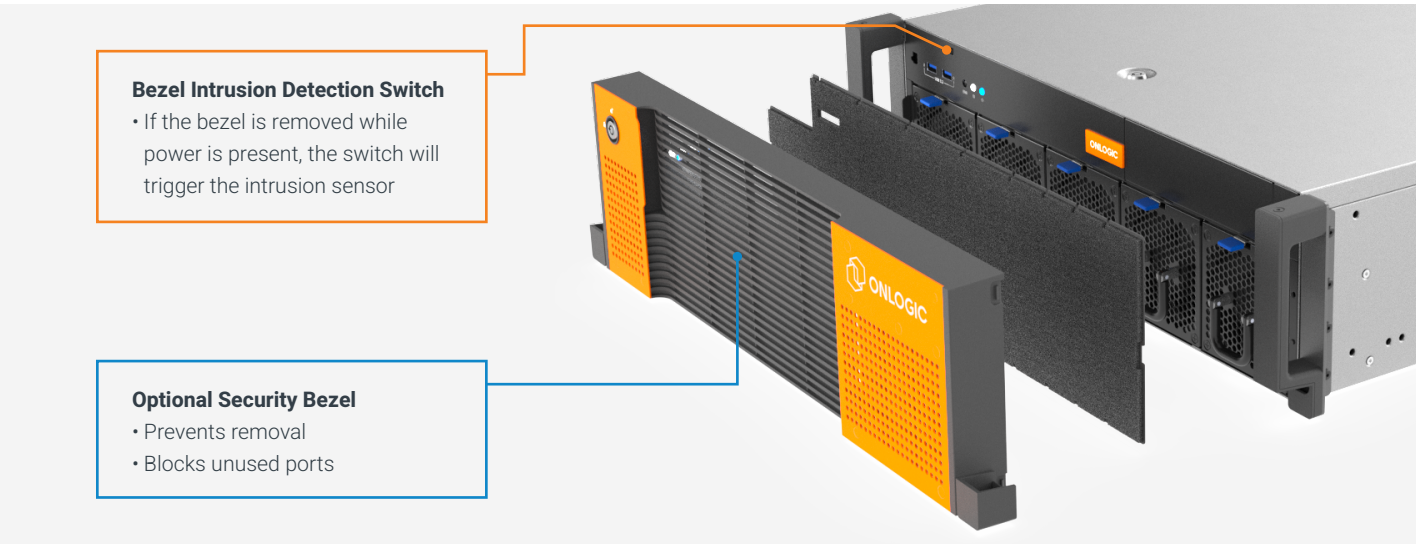
Device Security

As for edge devices, internal networks are still subject to physical attacks. Devices must be hardened to provide additional protection.

Physical Intrusion Prevention:

- Blocking Access to or disabling unused I/O
- Intrusion detection features when opening systems or enclosures
- Prevent cables from being removed
- Prevent systems from being removed from site. Lock servers to racks, use Kensington locks for workstations, enclose systems in the field.

Device security should be encompassed as part of a larger site security policy with access control, monitoring, and employee training.



Conclusion: The Power of Edge Virtualization

Virtualization at the edge is a powerful tool to manage legacy applications, create and deploy new applications, and develop a scalable edge environment. To take advantage of edge virtualization, the unique requirements of edge workloads must be considered. Platforms need to be resilient against failure and secure against cyber attacks — for mission-critical applications downtime is unacceptable. Together OnLogic and NodeWeaver combine reliable hardware with virtualization built for scaling at the edge. The OnLogic AX300 Edge Server provides a reliable hardware solution for applications including mass inference, model training, and high performance computing at the edge.

Ready to get started? Contact us!

Our team of experienced hardware specialists are here to help you select and customize your ideal computing platform. Reach out for a free project consultation.

North America

Call: +1 (802) 861 2300
Email: info@onlogic.com
www.onlogic.com

Europe

Call: +31 88 5200 700
Email: info.eu@onlogic.com
www.onlogic.com/eu-en/

1. Unlocking Performance: How Manufacturers Can Achieve Yop Quartile Performance
2. SensEye Predictive Maintenance: The True Cost of Downtime 2022
3. KnowBe4 Report Reveals Critical Infrastructure Under Siege with Cyber Attacks Increasing 30 Percent in One Year