How to unite modern and traditional at the industrial edge

Build a bridge between virtual machines and containers with Red Hat

Red Hat

ATS GROUP ADVANCED TECHNOLOGY SERVICES

Red Hat Advanced Business Partner

Table of contents

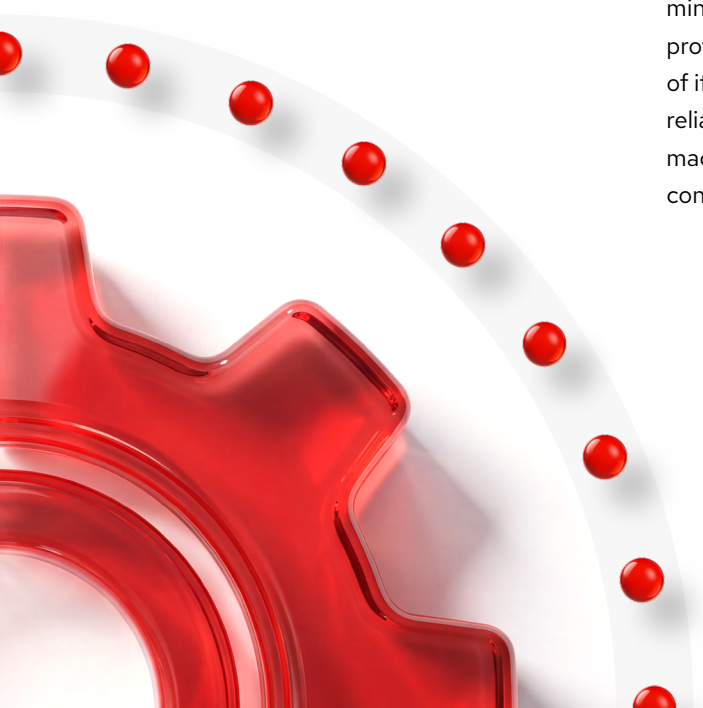
Introduction

The state of the edge

For decades, operational technology (OT) has relied on specialized and often bespoke virtualization solutions to keep factory floors running and power grids stable. However, the traditional market for virtualization is shifting. Costs are rising, support models are becoming increasingly unpredictable, and a general sense of market disruption is forcing leaders to reevaluate their long-term digital strategy.

The challenge is that maintenance in these environments currently involves heavy human interaction which lacks consistency, documentation of what's been done, and an easy path to resolution when things break. In OT, a system failure isn't just a lost transaction; it can represent a physical safety risk or a multimillion-dollar production halt. As a result, many organizations are relying on fragile, aging systems that are difficult to secure and even harder to scale.

Beyond technology, this transition is also about financial predictability. Red Hat provides a stable model by back porting patches, which provides consistency over upstream alternatives. That consistency helps leaders plan for long-term growth for both their traditional and modern workloads. This durable, open alternative bridges the gap. It's not just about replacing a hypervisor; it's about establishing a consistent platform across private datacenters, public clouds, and the furthest edge of the network. By prioritizing a safety-first, security-focused mindset, Red Hat helps organizations to prove their systems are safe regardless of if they are modern and provide a reliable bridge from traditional virtual machines (VMs) to the intelligent, AI-ready containerized edge of modern systems.



Reframing the OT/IT relationship for today's industries

The historical divide between IT and OT is often characterized by conflicting priorities: IT focuses on standardization, security, and auditability, while OT prioritizes operations uptime, safety, revenue and efficiencies. However, to scale for the edge in today's complex systems, these 2 worlds must find a common language.

The IT reality of an OT team's responsibilities

In reality, OT teams have been running sophisticated IT operations for years—managing bespoke servers and industrial PCs manually to make sure production never stops. The problem is that these tactical, isolated implementations are often difficult to extend or secure globally. By acknowledging that OT teams are already managing a complex range of industrial PCs, specialized controllers, and server-grade hardware, the conversation can shift toward providing them with enterprise-grade tools that act as a strategic accelerator. These tools professionalize and simplify their existing workload through automation and consistency, rather than adding new layers of complexity to their high-stakes daily operations.

Professionalizing the toolset

Modernization at the edge isn't just about the technology; it is about the methodology. Modern platforms provide enhanced capabilities—such as intent-based configurations and automated operational frameworks—designed to fit within specific industrial safety requirements. By treating Infrastructure as Code (IaC), organizations can make sure that updates are reviewable, reproducible, and easily reversible.

This approach also streamlines administrative hurdles such as audit readiness. By using automated reporting and version-controlled configurations, organizations can maintain continuous visibility, providing immediate proof of compliance and adherence to security standards. The transition from manual logs to automated reporting reduces the time and resources spent on regulatory oversight, moving away from manual, inconsistent configurations toward a standardized, automated approach that reduces human error and operational risk.

Delineation via software

One of the primary concerns in industrial environments is the potential for unauthorized or accidental interference with critical machinery. Traditionally, this was solved through network segmentation, but the need for real-time data makes physical isolation increasingly impractical. Modern software-defined platforms provide a solution through delineation via software. By implementing advanced access controls and logical partitioning, organizations can create defined boundaries with stringent security measures. This allows for autonomous management of critical workloads within specified platform constraints, bridging isolated team structures without compromising the safety of the plant floor.

Chapter 1

Facilitate incremental upgrades

The shift toward modern software architecture often presents a hurdle for industrial organizations. Many critical applications—frequently hosted on traditional Microsoft Windows or Linux VMs—are deeply integrated into operational workflows and cannot be easily refactored into containers without substantial risk and downtime.

Modern compute platforms serve as a future-ready bridge, allowing for a phased modernization strategy that avoids the high costs and operational disruptions of a complete, immediate rearchitecture.

Strategic migration for operational stability

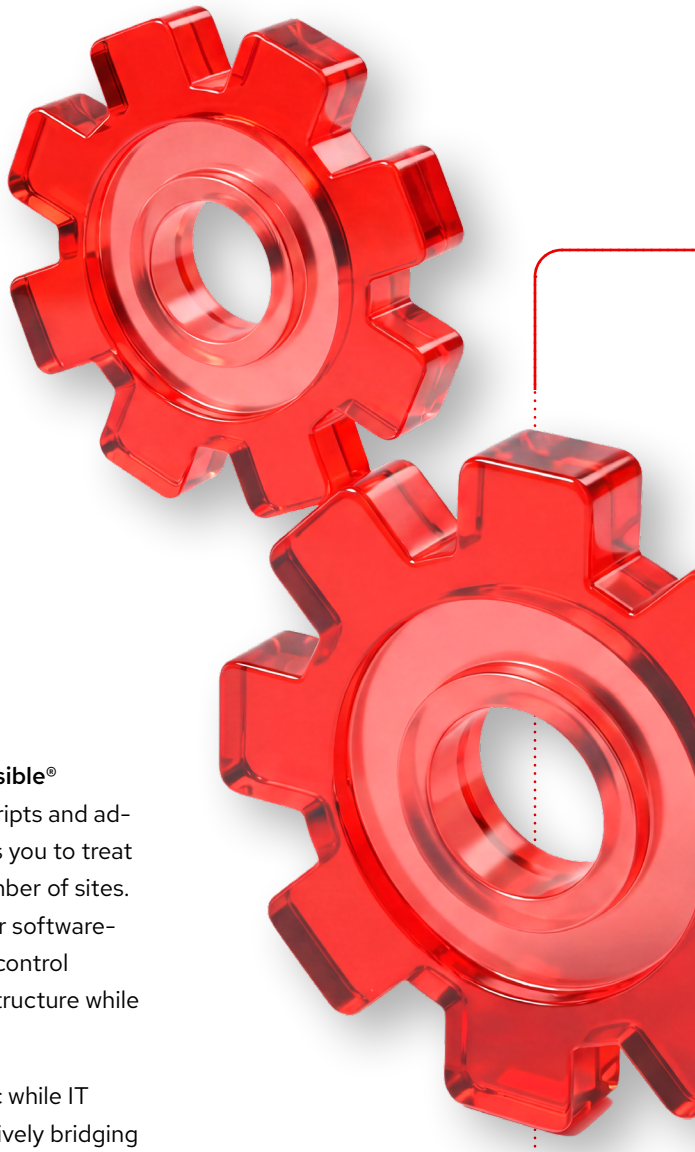
Operational stability is the primary requirement for edge deployments. Advanced virtualization capabilities within a modern orchestration layer allow for the migration of existing VM-based workloads to a standardized platform without altering the application code.

This modernize-in-place methodology helps organizations preserve investments in traditional software while immediately gaining the advantages of centralized management and improved security monitoring. By transitioning these workloads to a common compute layer, the reliance on specialized, proprietary virtualization hardware is reduced, freeing up resources that can be reallocated toward long-term innovation and intelligent edge capabilities.

Convergence of side-by-side operations

A platform that treats VMs as equal participants alongside containers within the same environment offers unique architectural advantages. These VMs function within the same context as containers, sharing a unified fabric of networking, storage, and administrative tools. This side-by-side operational model allows for the continued use of traditional applications—such as historical data loggers or human-machine interfaces—while simultaneously deploying new, edge-native microservices or AI models on the same physical hardware.

This convergence simplifies the edge footprint, reduces maintenance complexity, and makes sure that modernization occurs as an incremental evolution rather than a disruptive event. By consolidating all of this into a unified visibility layer, the platform provides holistic oversight of the entire environment through a consolidated monitoring interface.



Establish a unified foundation for intelligence

The primary objective of modernizing the edge is the transformation of raw data into useful intelligence. Historically, this data has remained isolated and fragmented across disparate VMs,disconnected physical devices, and proprietary monolithic systems.

By consolidating these compute resources onto a unified platform, organizations establish a consistent data layer across the entire enterprise. This consolidation is a prerequisite for advanced strategies, including predictive maintenance and autonomous edge operations. When traditional applications and modern analytics engines coexist on a single, integrated platform, the visibility of data increases, creating a sustainable path from traditional operations to the edge.

Using Red Hat to face these challenges

Standardization of operational workflows is realized through **Red Hat® Ansible® Automation Platform**, which allows organizations to transform manual scripts and ad-hoc IT practices into standardized, human-readable playbooks. This allows you to treat infrastructure as code, making configurations reproducible across any number of sites. For delineation, **Red Hat OpenShift®** provides the technical framework for software-defined isolation. By using namespaces and advanced role-based access control (RBAC), Red Hat OpenShift lets IT and OT share the same physical infrastructure while maintaining complete separation of duties.

This allows OT to maintain autonomous control over machine-critical logic while IT maintains the underlying platform to enterprise security standards, effectively bridging separated environments without compromising site safety.

Chapter 2

Extending lifecycles with both a safety and security focus

In industrial and critical environments, security is intrinsically linked to physical safety. A compromised system at the edge doesn't just result in a digital data breach—it can lead to equipment damage, environmental hazards, or direct threats to human life.

Modern architectural approaches give options—such as the ability to roll back if tests aren't passed with an update—to prioritize a safety-first security mindset. This helps make sure that platforms remain durable, stable, and compliant over exceptionally long operational lifecycles without requiring the frequent, disruptive updates common in standard IT environments.

Stability to promote both safety and security

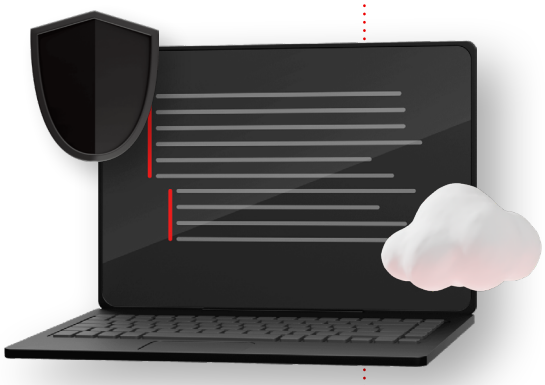
In industrial settings, a security update requiring a system reboot can be more of a disruption than a benefit. Operational priorities center on keeping the system running exactly as intended, as any unscheduled stoppage can have catastrophic consequences for production or safety.

By focusing on stability and predictability, a security-focused foundation honors the physical safety requirements of the site. This approach allows for the maintenance of operational integrity where layered security features protect the underlying data without interfering with the continuous execution of critical processes.

Hardware abstraction and sovereignty

Many traditional systems are tied to specific, aging hardware components, creating a precarious dependency on fragile supply chains and obsolete parts. Decoupling software from the physical layer through a consistent virtual hardware layer helps mitigate these risks.

This hardware abstraction makes critical workloads run on standard, commercial off-the-shelf (COTS) servers. By abstracting the software from the physical box, the operational logic remains intact and sovereign, delivering software that remains portable and functional even as the underlying hardware evolves or there are shifts in the vendor ecosystem.



The power of backporting patches

A primary requirement for industrial sectors is the availability of long-term support. Modernizing an edge site every few years is not feasible when the equipment it controls—such as turbines or manufacturing lines—may have a 20-year lifespan. Modern platforms address this by offering extended lifecycles that can reach up to 13 years of support.

A critical component of this longevity is the ability to backport security patches. This process involves taking critical security fixes from the latest software releases and applying them to the stable, older versions currently in the field. This delivers systems that stay aligned with up-to-date security standards against modern threats without the risk of "breaking changes" or forced upgrades that might destabilize production uptime.

The virtualization sandbox

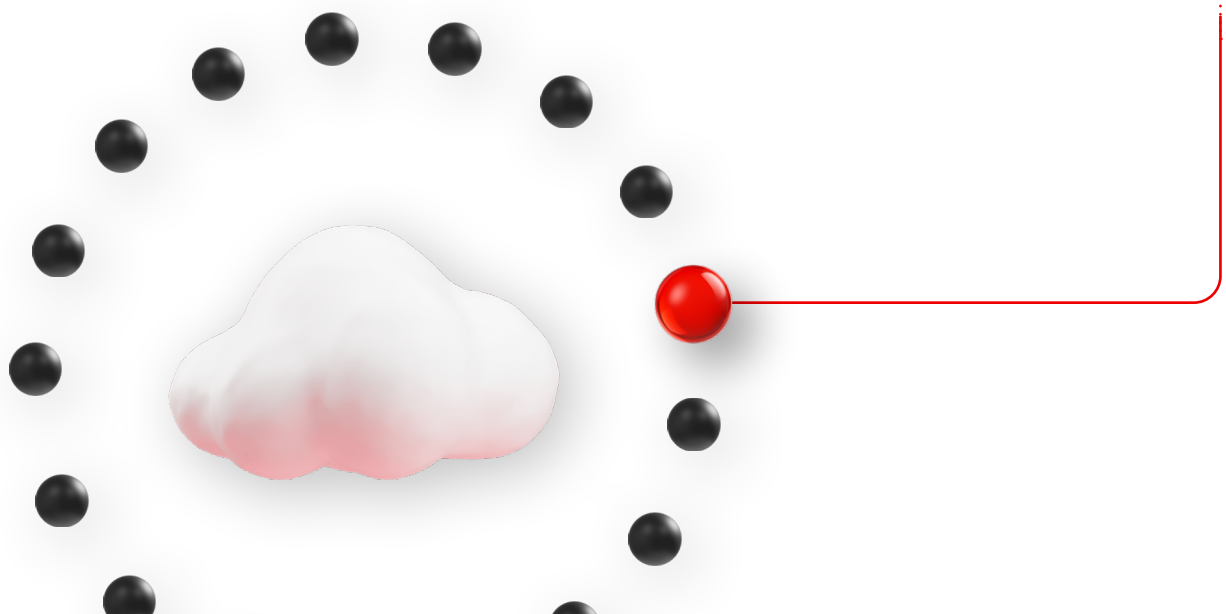
Traditional applications—some of which have been in operation for decades—frequently require specific, outdated operating system (OS) environments to function correctly. Converged compute environments allow these applications to reside in a virtualized environment next to microservices on a modern platform. This extends the operational lifespan of traditional software that is otherwise incompatible with contemporary hardware or modern security protocols.

By wrapping these unique, often highly customized configurations in a managed virtual environment, organizations can maintain their critical processes while incrementally building a modern, containerized future around them without a rip-and-replace requirement.

Using Red Hat to face these challenges

The technical cornerstone for this incremental approach is **Red Hat OpenShift Virtualization**. Red Hat OpenShift Virtualization, a part of Red Hat OpenShift, allows organizations to run traditional VMs alongside modern containerized workloads on a single, unified platform. By using the same trusted hypervisor found in **Red Hat Enterprise Linux®**, it provides a stable environment for critical applications that cannot be containerized.

This side-by-side convergence is supported by **Red Hat OpenShift** data services, which unify the storage layer for both VMs and containers. This integration allows data generated by traditional systems to be immediately accessible to modern analytics engines, providing the future-ready bridge required to evolve toward intelligent operations without a disruptive rip-and-replace of current workloads.



Chapter 3

Low-latency modernization and sovereign AI

As organizations move toward more intelligent edge operations, a barrier is often encountered that cloud computing alone cannot solve: the laws of physics. While the cloud is effective for massive data processing and model training, the realities of bandwidth, latency, and reliability at the edge require a more distributed approach.

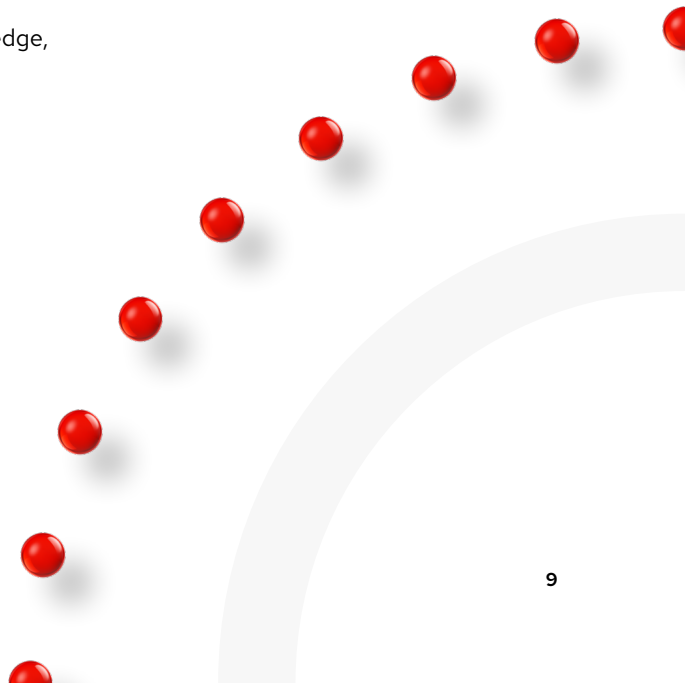
Physics over cloud

In a factory or on an energy grid, decisions often need to be made in milliseconds. Waiting for data to travel to a central cloud and back is not just inefficient—it can be impossible due to limited bandwidth or intermittent connectivity. Thus, a strategy is required that emphasizes processing data at the source. By running compute-heavy workloads, such as computer vision for quality control or real-time sensor analysis, directly on site, organizations can bypass network constraints and make sure that critical operations are never delayed by a slow connection.

Sovereign AI and operational autonomy

At the edge, sovereign AI is not a luxury; it is a tool for autonomy and reliability. Sovereign AI that is separate from a cloud-based central application programming interface (API) is required for quick operations on site. This level of autonomy is critical for resilience because if the network goes down, the edge site must remain operational.

By deploying AI models directly onto advanced compute platforms at the edge, organizations help make sure that their local operations remain sovereign, intelligent, and autonomous, regardless of external connectivity, or the downtime of AI service providers.



Edge-optimized footprints with lightweight orchestration

Not every edge location has the space or power for a full server rack. For resource-constrained environments—such as industrial controllers, field devices, or drones—lightweight, enterprise-grade orchestration solutions are required.

These are specifically designed for small footprints. With minimal requirements of just 2 cores and 2GB of random-access memory (RAM), these edge-optimized solutions allow organizations to extend modern, containerized workloads to the furthest reaches of their operations without sacrificing the enterprise-grade stability and support required for industrial success.

Using Red Hat to face these challenges

Red Hat's build of **MicroShift** provides a lightweight Kubernetes orchestration solution that brings full enterprise capabilities to small, resource-constrained devices. As part of **Red Hat Device Edge**, MicroShift helps implement sovereign AI by helping complex models run locally, providing autonomy even during network outages.

For broader consolidation efforts, **Red Hat OpenShift** provides the high-performance environment needed to virtualize and consolidate dozens of physical controllers into a few software-defined nodes. This entire architecture is underpinned by **Red Hat Enterprise Linux**, with the same hardened foundation used in the datacenter as at the furthest reaches of the network, whether on a massive server or a 2-core controller.

Chapter 4

Improve reliability

In the world of OT, reliability is the baseline for all innovation. If a system is not reliable, it cannot be considered safe. Enterprise platforms provide multiple layers of technical resilience to support edge deployments through hardware failures, network outages, and unsuccessful updates without human intervention.

Flexible high availability for every site

Traditional high-availability (HA) configurations often require a massive compute footprint, which is cost-prohibitive for smaller edge sites. Flexible HA options are designed to match the specific needs and budgets of industrial locations. While a full 3-node cluster provides maximum resilience, support for 2-node plus arbiter configurations allows for a smaller, lower-cost witness node—which could be virtualized on site or on smaller resource-constrained hardware—to act as the tie-breaker to maintain quorum. This significantly reduces the expenditure for smaller sites while still providing enterprise-level failover and redundancy.

Zero-touch self-healing with automated rollbacks

Updating software on a device in a remote or hazardous location carries the risk of failures that could render the unit inoperable while it is inaccessible. Automated self-healing processes mitigate this risk. When a device receives an update, a modern unified platform executes a series of health checks. If the system fails to boot correctly or the critical application doesn't start as expected, the system automatically rolls back to the last known good state. This zero-touch recovery makes sure that a failed update doesn't result in a manual intervention or an extended production halt.

Using Red Hat to face these challenges

Resilience is hard-coded into the architecture through Greenboot, a health-check and self-healing framework within **Red Hat Device Edge**. Greenboot ensures that any unsuccessful update to **Red Hat Enterprise Linux** or the resident applications triggers an automatic rollback, preventing remote devices from becoming inoperable. For site-wide reliability, Red Hat OpenShift allows for flexible high availability through 2-node clusters using an external arbiter, providing a durable failover mechanism with a minimal hardware footprint.

Chapter 5

Streamline operations and fleet management

The scale of the edge presents a unique management challenge. Managing 5 servers in a temperature-controlled datacenter is vastly different from managing 5,000 devices across remote industrial sites. Modern toolsets provide the capabilities necessary to move from manual, ad-hoc maintenance to automated, fleet-wide operations.

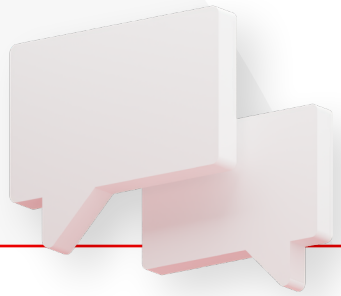
The mindset shift: From bespoke to standardized

In traditional IT, servers are often bespoke—individual machines that are manually named, patched, and cared for. At the edge, this model fails. Organizations must adopt a fleet mindset, in which thousands of devices are treated as a single, collective entity. This shift requires a standardized approach to provisioning and updates.

With a centralized platform with broad automation capabilities, an administrator can define the desired state for an entire class of devices and allow the system to handle the deployment. This move from individual management to fleet-scale orchestration is the only sustainable way to maintain consistency and security as edge footprints grow.

Centralized fleet management

The cost of maintaining remote edge sites is largely caused by required manual on-site visits when things break. This manual intervention is slow, and can be a vector for vulnerability and stability issues due to bespoke one-off fixes. Centralized management tools that have unified data and process it for insights change this dynamic by providing visibility and proactive control. Instead of waiting for a site to fail, potential issues can be identified from a single dashboard before they cause downtime. By treating 10,000 devices as a single entity, zero-touch provisioning and intelligent over-the-air (OTA) updates are possible, making sure that security patches and application improvements are delivered efficiently without manual intervention.



Automation at scale: Unifying operations

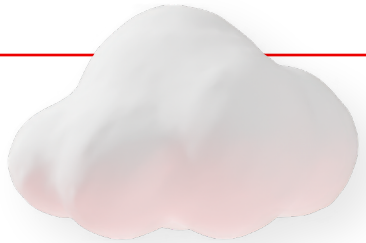
True operational excellence at the edge requires a unified approach to automation. Combined automation and cluster management solutions work together to unify Day 2 operations from the core datacenter to the furthest edge. While automation handles the OS and infrastructure tasks, multicluster governance provides the oversight needed to manage diverse workloads.

This unified toolset allows teams to use familiar skills and workflows to manage the entire lifecycle of edge devices—from initial deployment to decommissioning—providing intelligent edge environments that are durable and security-focused, with streamlined operations.

Using Red Hat to face these challenges

The transition from individual device maintenance to fleet-scale management is powered by **Red Hat Edge Manager**, which provides a central console to monitor and update thousands of distributed devices simultaneously. This capability is integrated with Ansible Automation Platform, allowing administrators to deploy complex application updates or security patches using human-readable automation across the entire fleet.

For multicluster governance, **Red Hat Advanced Cluster Management for Kubernetes** provides a unified dashboard to manage both core datacenter and edge clusters, making sure that security policies and operational standards remain consistent regardless of where the device is located. This unified management stack eliminates the need for manual on-site visits, replacing expensive truck rolls with efficient, centralized orchestration.



Chapter 6

Architectural pillars for a consistent edge strategy

A successful transition to the intelligent edge is built upon a foundation of integrated technical capabilities. These pillars work together to solve the challenges of maintaining traditional stability while supporting modern, data-powered innovation.

Red Hat provides the essential infrastructure components to realize this strategy, delivering an architecture that is cloud-consistent but edge-optimized.

The enterprise-grade foundation: Red Hat Enterprise Linux

A consistent OS serves as the primary anchor for the entire distributed ecosystem. Red Hat Enterprise Linux provides the hardened, security-focused base required for industrial operations. By using image mode for Red Hat Enterprise Linux, organizations can deliver the OS as a container image, allowing every device in the fleet to run a bit-for-bit identical environment. This eliminates the risk of configuration drift and simplifies the deployment of security patches. The Red Hat Enterprise Linux has a long-term support model, which prioritizes stability through backporting critical fixes.

Unified container and VM orchestration with Red Hat OpenShift

A single orchestration layer simplifies the operational environment by managing traditional VMs and modern containers side-by-side. Red Hat OpenShift, using OpenShift Virtualization, brings virtual machines into the Kubernetes-native fold.

This convergence eliminates the need for isolated management structures and allows for a “migrate now and modernize later” strategy. By running traditional workloads in the same context as modern microservices, organizations can establish a unified data fabric, which is the essential prerequisite for deploying advanced analytics and edge-based intelligence.

Lightweight orchestration for resource-constrained locations with the Red Hat Device Edge

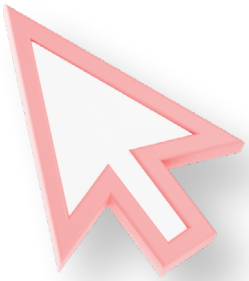
Operational environments frequently include locations where space, power, and thermal constraints make full-scale servers impractical. To extend intelligent capabilities to the furthest reaches of the network—such as industrial controllers or field sensors—Red Hat's build of MicroShift provides a lightweight orchestration solution.

As a component of Red Hat Device Edge, MicroShift is specifically optimized for small footprints. This makes sure that maximum system resources are dedicated to the operational workload rather than the platform itself, all while maintaining complete operational parity and security standards with larger central Red Hat OpenShift clusters.

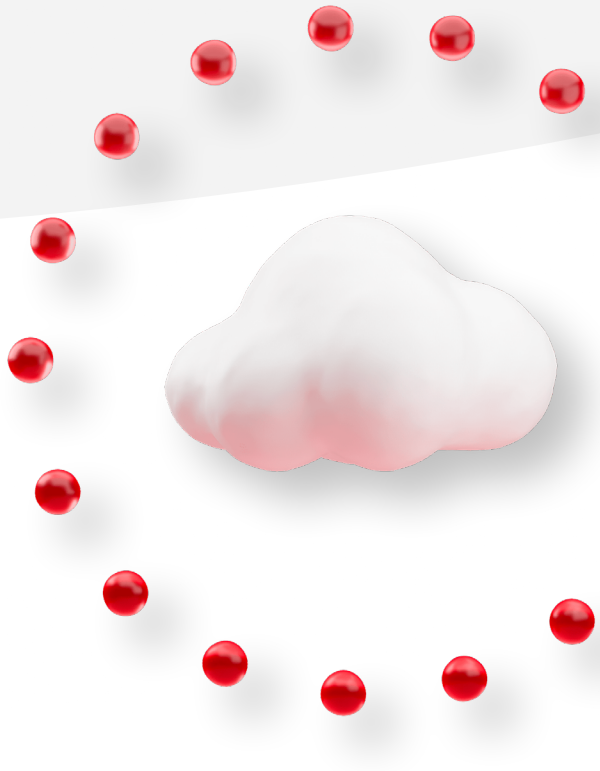
Standardized automation and governance with Ansible Automation Platform and Red Hat Advanced Cluster Management.

Managing thousands of remote devices requires a move away from manual interventions toward standardized automation. Red Hat Ansible Automation Platform provides the framework to automate everything from the OS to the application layer using human-readable templates.

Working alongside Red Hat Advanced Cluster Management and Red Hat Edge Manager, these tools provide the centralized governance needed to manage the entire lifecycle of edge devices. Furthermore, by treating infrastructure as code, organizations achieve a level of audit readiness that simplifies compliance with industrial safety and regulatory standards.



Conclusion



The durable alternative

Modernizing the edge is a strategic journey balancing stability and innovation. An open, durable alternative to proprietary systems provides a sustainable bridge to the intelligent edge.

Next steps

Begin your journey by attending our webinars to explore real-world industrial innovation.

Register for a webinar

Explore the Red Hat edge portfolio

Appendix:

Proof points and real-world uses

Modernization is best understood through its results. These case studies illustrate how advanced compute platforms are solving complex edge challenges today.

Tanobel protects traditional investments while modernizing

Through adopting Red Hat OpenShift Virtualization, Indonesian water manufacturer Tanobel successfully modernized its traditional infrastructure to support rapid business growth and strict regulatory compliance. The transition allowed the company to consolidate 90% of its workloads into containers while maintaining essential traditional applications and databases as VMs on a single unified platform. This modernization effort improved operational efficiency, reducing the execution time of critical daily jobs from 1 hour to less than 10 minutes.

Read more →

Hisense speeds processes with Red Hat solutions

Hisense implemented a containerized cloud platform using Red Hat OpenShift and Red Hat Consulting services. Facing challenges with bulky traditional systems, the electronics leader adopted a Platform-as-a-Service (PaaS) architecture to automate environment setups and streamline application delivery.

Read more →