White Paper

A Modern Alternative to VMware and Legacy Hardware Procurement

RGS
Rancher Government Solutions

Table of Contents

Legacy Systems: Compounding Challenges for Government IT

Traditional infrastructure solutions have been the backbone of government IT operations for decades. However, they often come with heavy hardware dependencies and are not built to manage both containers and virtual machines efficiently. This limitation becomes apparent as government and military operations seek to modernize their IT environments to be more flexible and scalable.

Legacy IT infrastructures, like VMware's vSphere/VCF, are increasingly becoming bottlenecks for organizations trying to stay competitive and responsive. The recent acquisition by Broadcom has only amplified these challenges and drawn attention to the inherent limitations of legacy systems. Plagued by high operational costs, inefficiencies, and rigid architectures, these systems compromise scalability and security by:

Escalating Costs

Maintenance of outdated hardware and software requires significant resources.. Organizations are often burdened with increasing licensing fees and maintenance costs as these systems age, which can strain budgets and drive funds away from innovation. The acquisition-induced uncertainty may increase costs as new pricing models are adopted.

Operational Inefficiencies

Legacy systems are proving too complex to update and maintain, usually requiring extensive manual processes that increase the likelihood of errors and downtime. This complexity can halt your operational efficiency and make it even more challenging to adapt to new requirements or tech advancements in the long run.

Lack of Flexibility and Scalability

Legacy systems often operate in silos with limited compatibility with new technologies, making integration a significant challenge. The rigid nature of these systems means government and military organizations can't scale operations as quickly and efficiently as needed. This becomes problematic as government and military operations require integration with advanced analytics and real-time data processing technologies. Because traditional infrastructures can't quickly scale up or down, they struggle to meet the scalability demands of critical missions without significant capital investment and operational disruptions.

Security and Compliance Risks

Legacy systems fall short of modern security compliance standards, exposing operations to increased cyber threats. As security standards become more stringent, older systems may not receive updates fast enough to address new vulnerabilities, putting critical mission data and operations at risk.

Forced Obsolescence and Vendor Lock-In

Many legacy systems are built on proprietary technologies that lock organizations into specific vendors. This dependency results in a lack of control over infrastructure and can force agencies into costly and unnecessary upgrades.

Many government IT teams seek flexible and efficient alternatives to traditional solutions like VMware's vSphere. As government and military operations' needs grow, so does the demand for systems that can seamlessly integrate containers and virtual machines (VMs) within a unified framework.

Rancher Government Harvester: A Legacy System Alternative

Rancher Government offers a modern alternative to legacy hardware systems holding government and military operations back. In contrast to traditional platforms such as vSphere, Harvester is a modern hyper-converged infrastructure (HCI) product that is purpose-built to run containers and virtual machines under a unified management framework by using Kubernetes as the orchestrator and lifecycle management platform. It also combines all infrastructure services including block storage, software-defined networking, load-balancing, and vGPU. It is an open source product decoupled from hardware dependencies (outside of CPU architecture requirements) and can be installed easily using a simple menu-driven ISO install or PXE-booted automated install.

Being open source and open-standards-based means Harvester is highly flexible in working with other open source and open-standards applications and tools, especially those that target Kubernetes environments. Harvester's true power comes from leveraging the open source community of software that allows it to be the true catalyst for a better-together solution in your infrastructure capable of building targeted solutions without stretching scope.

Rancher and Kubernetes Cloud: On-prem Edge

The entire Rancher stack addresses the unique needs of government and military operations but maintains an open source and open-standard policy, making it exceptionally flexible and adaptable with other software. Unlike all other Rancher products, Harvester sits at the infrastructure layer and is natively compatible with other Kubernetes applications and tools, many of which are in our certified integration application catalog. Unlike traditional infrastructure like VMware, many of the services available can run within Harvester's own Kubernetes-based cluster, which drives more flexibility and functionality than legacy systems.

Take, for example, the use case of running HashiCorp's Vault within the Harvester cluster. There is now an infrastructure-level service providing secret storage and management so that all VM and container workloads can use it for storing secrets immediately. In traditional infrastructure, you would be forced to spin up a set of heavier VMs for high availability and manage them with VM automation tools that would need to be also installed and configured.

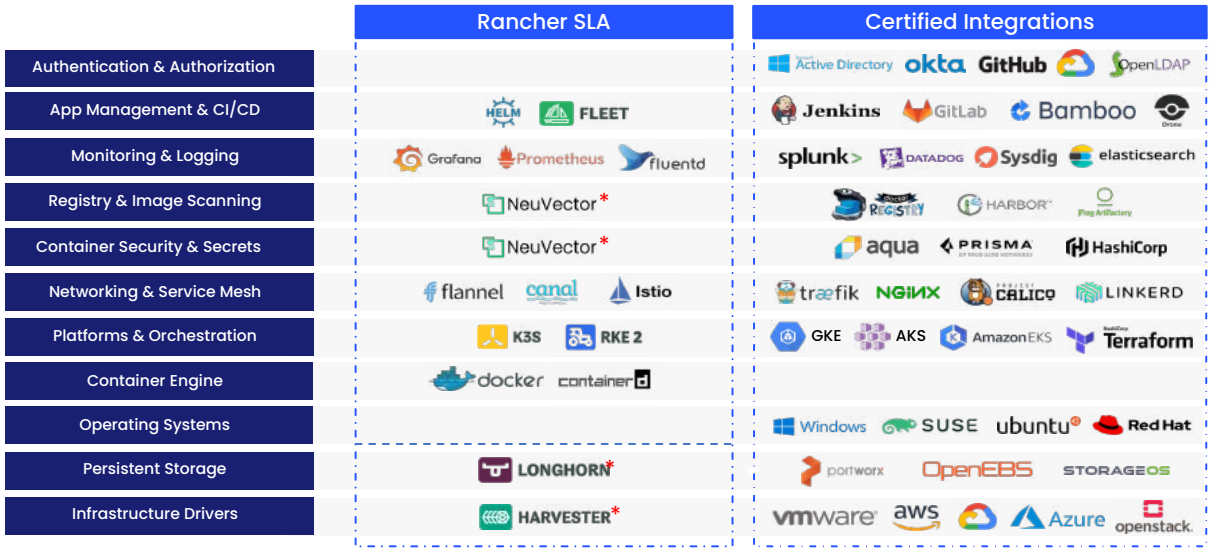
Because Vault is already running in Kubernetes containers on Harvester, the built-in lifecycle management utility already exists, which reduces the resources needed to run, manage, and automate this process. This process can be replicated across other services, such as Keycloak, Harbor, Kasten, and GitLab, to simplify your infrastructure footprint.

When coupled with the Rancher Multi-cluster Manager (MCM) as the management plane, you unlock new features within Harvester with strong UI and power-user interfaces via the Kubernetes API, including:

- Define and manage RKE2 clusters as helm charts
- Robust RBAC backend supporting different authority providers
- Powerful GitOps/CD tool in Fleet with certified support for Argo and Tekton
- Strong logging operator based around Fluent
- Metrics and observability features via Grafana Labs

In addition to all these features, Rancher MCM allows you to use your preferred tools as a replacement, never locking you into pre-selected features. With Kubernetes under the hood, Harvester inherits a unified language and API that can describe all workloads, processes, and resources running within an entire environment. Kubernetes' ability to transform cloud-specific components into cloud-agnostic objects includes containers, storage volumes, virtual machines, networks, and more.

The power-user and automation potential is a quantum leap over other solutions on the market. And these features of automation are nothing new to learn, they are already industry standard; if you are running GitOps in your Kubernetes environments, those same processes translate directly to running and managing on Harvester.



** Additional support subscription required.*

Capability Matrix

While the Kubernetes-based nature of Harvester means it does not match up one to one with vSphere, there are some similarities. And with the entire Rancher stack available to support Harvester, a more well-rounded matrix emerges.

Harvester is comprised of eight major components:

1. Virtualized Compute via KubeVirt
2. Scalable, networked block storage via Longhorn with support for 3rd party providers
3. Cluster/DC Management via Rancher MCM
4. Network segmentation and isolation support via Multus and NetworkPolicy
5. Full SDN w/ IPAM support via Multus
6. Load Balancing (Layer 2 or BGP) via Kube-VIP
7. Secure-by-default Container Orchestration via RKE2
8. Secure, Immutable Operating System via SLE Micro / Elemental

To see how this stacks up with vSphere, we've highlighted components included within Harvester:

Capability	Harvester	vSphere
Virtualization	Kubevirt	ESXi
Storage	Longhorn	vSAN
Management	Rancher MCM	vCenter
Cluster Management	Rancher MCM	Tanzu Mission Control
Networking	Multus + Canal	vCenter + NSX-T
Load Balancing	Kube-VIP (L2 & BGP)	NSX-ALB (Avi)
Container Orchestration	RKE2	TKGs / Workload Mgmt
OS Layer	SLE Micro + Elemental	Photon
Ops Management	Rancher MCM + Monitoring	Aria
GitOps Automation	Fleet/Flux/Argo/Tekton	Tanzu Automation
Service Mesh	Istio, Consul, etc.	Tansu Service Mesh*

** Only available within AWS multi-cloud footprint*

Virtual Desktop Infrastructure

Another everyday use case of VM-based infrastructures is providing Virtual Desktop Infrastructure (VDI), the lifecycle management, access, compliance, and security of workstations hosted virtually on top of your infrastructure, whether on-prem or in the cloud.

VMware Horizons or Citrix-based desktops are both hosted with a tightly coupled solution in vSphere. Using other infrastructures in their place, especially more modern ones like Harvester can be difficult or may cause a loss of standard features. Other options like Horizon have been spun off and sold to KKR, a consortium. KKR's strategic plans for its software product are not well known. They may not follow industry trends, making adopting this alternative solution or renewing their licenses with KKR risky.

Harvester's open source and open-standard fundamentals enable it to leverage all other tools in the industry, and VDI is no exception. This flexibility becomes a serious value-add and a great improvement over existing VDI solutions on the market.

KASM

Enter KASM, an infrastructure-agnostic approach to VDI that leverages modern development tools and patterns to deliver high-quality virtual desktops via web browsers and thin-clients. KASM's core capability embraces container-driven development that runs equally well within VMs or as containers. Because of this, KASM can also run container-based virtual desktops, a stark difference from the current industry's usage of VMs. Container-based virtual desktops use a mere fraction of their VM counterparts resource footprint and are able to be provisioned and scaled much faster.

RGS has partnered with KASM to deliver KASM capabilities onto Harvester as an emerging on-premise flagship VDI platform. As part of that development, Harvester's container-based orchestration has made some compelling use cases, deploying within seconds into Harvester with a Helm chart and the ability to be airgapped easily using Hauler.

Harvester can run containers on bare metal server hardware without needing an additional Kubernetes cluster, which works well with infrastructure-based services such as container registries and git repositories. Now, as a VDI broker, KASM fares well here. Because virtual desktops can now support both virtual machines and container hosts, the footprint for these virtual desktops is freeing up significant compute, memory, and space.

KASM's container capability means it can host virtualized apps without a whole desktop environment. This feature can help bypass the need for Windows or specific Linux-flavor VMs, especially regarding IDEs and QA testing. Instead, the apps can run directly, making the host OS layer irrelevant. With many VDI sessions being Google Chrome or Mozilla Firefox sessions, those apps are available out of the box.

KASM is purpose-built to be ready for the government customer on day one and has seen strong adoption across the DoD. While many customers working with the cloud use it within AWS or Azure, it runs equally well on Harvester for a proper on-prem and airgap-capable solution. This solution enables low-latency workstation enablement in any theater, regardless of a connection back to WAN.

The Rancher Government Difference with Harvester

The US Government requires specialized solutions tailored to its organizations' and mission partners' stringent compliance and airgap requirements. Rancher Government enhances the best of the Rancher upstream with our secure software supply chain solution, Carbide, providing hardened and security-capability enrichments for high-compliance environments and tactical applications.

Upcoming Features of Harvester as a specialized Carbide product release:

- FIPS-140-2 support at both Operating System & Kubernetes layer
- US-Soil built Harvester software assets and digitally signed container images with SLSA-3 Secure Supply Chain Compliance
- STIGATRON Day 2 Compliance Operator support for both Harvester-hypervisor and downstream RKE2 Kubernetes clusters
- Experimental Encryption-at-rest for Harvester VM Volumes & CSI Persistent Disks
- Harvester DISA STIG compliance out of the box (ISO installs only)
- Kubewarden Security Policy Engine
- UI Improvements & Carbide Branding
- Embedded Docs for disconnected knowledge management

Note: The features described above are exclusive to customers of Rancher Government and are not included in the upstream Harvester release.

Harvester Parity Opportunities

While there are several features some VMware customers use beyond the typical vSphere environment, there are alternatives within the Kubernetes ecosystem or general VMs that Harvester can provide. However, it's important to consider features and ensure they are being used with the primary use case in mind, as many customers find dropping these infrequently used features can greatly enhance the ease of implementing an alternative. These features include:

- **NSX-T:** A true Layer-7 SDN that ties into the vSphere ecosystem to provide tenanted, virtual private clouds with granular control. Issues with this feature include:
  - Difficulty in installing and requires significant hardware resources to run.
  - Many customers leveraging this capability do not need the scale of SDNs it provides.
  - Large organizations may use this to run their own on-prem clouds for numerous teams and applications with varying levels of self-service enabled.

  Solution: NetworkPolicy and MultipleNetworkPolicy within Kubernetes can provide strong ingress/egress firewall control via policy without the massive overhead. Combined with the new IPAM addon, Harvester becomes a fully-secure private cloud.

- **Backups:** Much of the government IT industry uses Veeam as its backup and recovery solution. However, this solution does not need to run solely on legacy infrastructure.

  Solution: Veeam's Kubernetes-focused backup solution, Kasten, works natively with Harvester's RKE2 baseline, allowing for an easier transition to a more modern infrastructure with reliable backup and recovery capability.

- **VM Migration:** In some infrastructures, customers have amassed a set of virtual machine template images. Issues with this include:
  - Templates are often used in a golden image pattern where they are approved and STIG'd; however, migration of these VM templates would need to occur as a running machine and, as a result, become stateful.

  Solution: Harvester includes the guestfs tools with libvirt for importing running VMs from a vSphere or OpenStack environment, which makes the process simple and beneficial. For scaling needs of this process or when configuration-as-code is needed for migration, using HashiCorp's Packer tool within Harvester can be an alternative as Harvester's VMs are run within secure Pods that have native QEMU support, eliminating the need for additional tools to construct a VM programmatically.

- **GPU Live Migration:** While Harvester supports live migration of VM workloads from node to node with the same CPU architecture, it does not support GPU-backed live migration. Currently, no known option exists to solve this problem at the infrastructure layer.

Licensing and Subscription Considerations

Licensing has seen a significant change following VMware's acquisition by Broadcom. Before the acquisition, VMware had a range of product offerings that competed with each other. While Broadcom has attempted to streamline these options, they have done so only with the largest partners in mind, sidelining smaller organizations' needs.

Securing a subscription quote under the new framework—specifically the VMware Cloud Foundation (VCF)—can take up to three months as of Spring 2024. VCF consolidates most of VMware's products and is heavily promoted as the go-to multi-cloud solution for platforms like AWS and Azure. However, this approach introduces additional layers of complexity and costs, complicating the management of cloud resources and escalating overheads for users.

In contrast to VMware's model, Rancher's billing is straightforward, emphasizing simplicity and predictability. Rancher's traditional billing is based on horizontal compute resources, meaning the costs are associated with the node count rather than the type or size of the VM. This model applies across various components such as RKE2, NeuVector, and Longhorn, treating each node as a bucket of resources, simplifying scaling and budgeting.

Rancher MCM has a transparent pricing model with a fixed cost for the first instance and discounts for additional cases. Typically, MCMs are used per isolation environment (unclass, secret, instance), but if there is network connectivity, one MCM manages all resources under that environment. This straightforward approach benefits organizations managing isolated environments or needing extensive network connectivity, as it allows for predictable budgeting and resource allocation.

Harvester introduces an even more flexible model, particularly beneficial for diverse environments spanning data centers to edge devices. It is billed per physical core and sold in packs. This core-based billing is also a bucket of resources that spans all bare-metal devices connected in a Harvester cluster, regardless of how they are divided across server racks, data centers, or regions. There is no licensing server or reachback/auditor running.

Given the stark differences in licensing models between vSphere and Rancher, working with a Solutions Architect is advisable. These experts can break down unique needs and identify the most efficient solutions for both functionality and horizontal compute at the right rate.

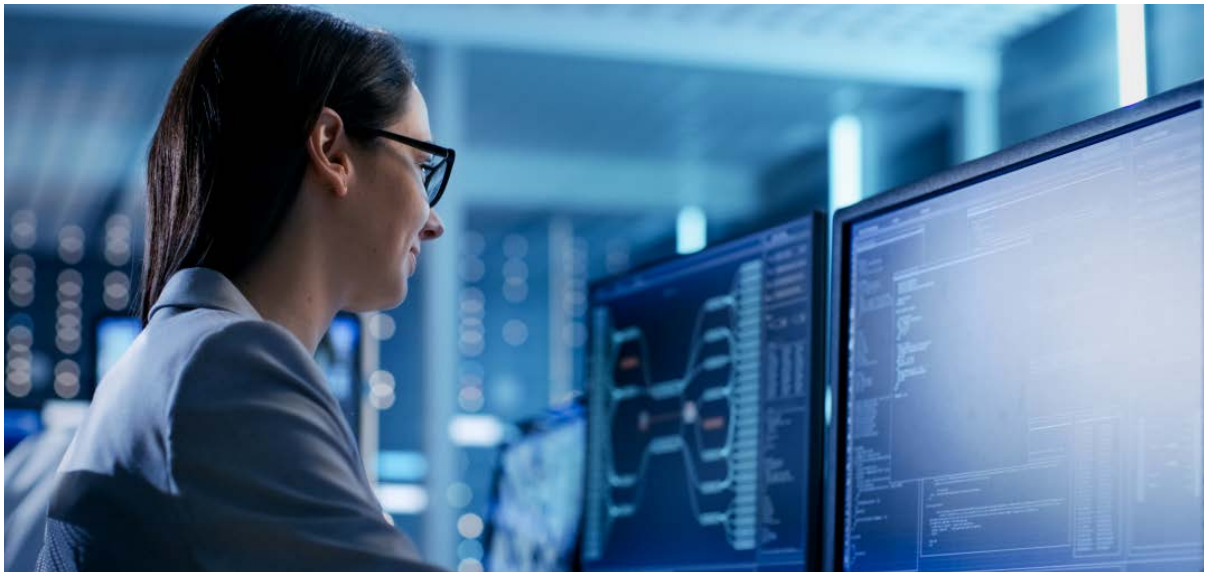
Advantages of Harvester for Government Operations

Advancements in cloud-native technologies and automation have outpaced the capabilities of many legacy systems, meaning there isn't always a direct comparison between old and new solutions. In some cases, Harvester may lack the specific features found in traditional solutions like VMware. However, this reflects that the industry has moved toward more innovative solutions that traditional models just can't provide.

Harvester introduces a new approach by integrating deeply with Kubernetes and offering a robust platform that excels when traditional infrastructures falter. Being open-source and adhering to open standards, Harvester is more adaptable in working with third-party solutions within the Kubernetes and Cloud Native Computing Foundation (CNCF) space—an area where VMware falls short.

This flexibility also extends to hardware compatibility, with Harvester capable of operating on a diverse range of equipment, like VxRail servers and older hardware collecting dust in a closet. Decoupling hyperconverged infrastructure from hardware dependencies can open up the reuse of existing hardware patterns and help reduce or remove blockers from hardware procurement lead times.

Finally, standardizing infrastructure management by using Kubernetes as a universal language across all elements, whether containers or virtual machines, allows for greatly reduced infrastructure code. Reduced complexity means easier maintenance, faster upgrades, more enhancements, and faster onboarding. Transitioning to a real, modern on-prem infrastructure opens up many usage and consumption patterns for engineering and operations teams.



Migrating to Harvester

Unlike traditional vendors' typical rip-and-replace migration methods, migrating from VMware to Harvester involves shifting an entire environment to run on top of a different infrastructure. While this can be a disruptive process and vary widely from customer to customer, the inherent multi-cloud capabilities of Rancher's suite of products, cloud-native tools, and VM migration add-ons means this process is broken down into a phased approach. Additionally, Harvester can coexist with vSphere environments seamlessly, making hybrid applications a feasible solution.

At a high level, we find two primary migration patterns with customers: VM migration and container migration. Knowing the functionality of the workloads is essential in cutting through the confusion.

As with all things Rancher, Kubernetes is under the hood, making the level of automation achievable without the UI involved in the process very high. Automated migration of similar workloads can also be an easy process when using automation tools and scripts that leverage Rancher and Kubernetes APIs.

VM Migration

Migrating VMs from vSphere to Harvester is straightforward, with a specific add-on tool crafted and curated for this exact use case—the VM Import Controller. When installed, this add-on tool can peer into your vSphere environment to fully migrate your VM and attached volumes into Harvester.

As part of this migration, you can define the mapping of vSphere-based networks to Harvester networks. Once the VM has been migrated to Harvester, you can export and save it to a base image that can be replicated or tied into infrastructure tooling like Terraform/Ansible.

Container Migration

There are a few ways to manage containers:

1. For customers opting to keep their vSphere containers as simple Docker containers running on a VM host, those containers would be automatically captured in the VM Migration approach.
2. Customers using RKE2 or K3S clusters within vSphere can leave them be, import them to Rancher MCM, or continue backing them up and restoring the clusters onto Harvester using Kubernetes backup solutions within our certified integration matrix, such as Kasten or Velero. Rancher MCM can also be migrated from vSphere to Harvester using the Rancher Backup Operator.

3. Customers using other Kubernetes distributions, such as TKGs or Workload Management, can import those clusters into Rancher MCM and manage them directly. Migrating these clusters may require extra steps as TKG uses a non-industry standard for managing packages and applications. Migrations here must be based on specific migration needs per application or copying the persistent volumes and deploying the same applications onto a new RKE2 cluster with the exact specifications. Migrating applications from these clusters may be an easier route.

All of these working patterns can be employed when migrating your infrastructure. With adequate planning, any downtime or disruption to operations can be minimized or eliminated. We suggest working with a Rancher Government Solutions Architect to plan this process, as every environment is unique.

Harvester Roadmap: Charting Next Steps

Our goal is to meet our customers at their mission and drive the Harvester HCI Edge platform closer to the bespoke needs of the government community. Below is a subset of features we are adding to enable every government mission to have highly available compute, anywhere.

v1.3.0 (Mar 2024)

- **vGPU** support for AI/ML-enabled Edge HCI
- **ARM64** Support (technical preview)
- Optimize for Frequent Power-off/Power-On operating procedures
- Two nodes (with witness) support
- Advanced Virtualized Networking with onboard DHCP
- GitOps-driven Fleet management for Harvester (technical preview)
- Thunderbolt tunneling and pass-through enabled

V1.4.0 (Fall 2024)

- **ARM64** Support (Experimental)
- GitOps-driven Fleet management for Harvester (Experimental)
- 3rd party storage providers now supported for VM root volumes
- Support shared storage for VM workloads
- Harvester Complete Cluster Backup
- Provide recurring backup for Virtual Machines and Volumes
- USB Passthrough
- Harvester Support Disaster Recovery Volumes
- Third-party Backup Solution support
- Harvester third-party storage support for diskless servers
- CPU Pinning

Schedule a demo to learn more about our Harvester HCI Edge platform and how we are enabling mission success at the tactical edge.

About Rancher Government Solutions

Rancher Government is designed specifically to address the unique security and operational needs of the U.S. Government and military as it relates to application modernization, containers, and Kubernetes.

Rancher is a complete open source software stack for teams adopting containers. It addresses the operational and security challenges of managing multiple Kubernetes clusters at scale while providing DevOps teams with integrated tools for running containerized workloads.

Rancher Government supports all Rancher products with U.S.-based American citizens currently supporting programs across the Department of Defense, the Intelligence Community, and civilian agencies.

To learn more about Rancher Government's products and solutions visit www.ranchergovernment.com

Info@ranchergovernment.com

844-RGS-7779
ranchergovernment.com
1900 Reston Metro Plaza
Suite 600
Reston, VA 20190