

Post-VMware Protection

Thank you for your interest
in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASPO ValuePoint, The Quilt and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Bacula Systems, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.



To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com



Explore More Resources:
carah.io/BaculaSystemsResources



Join Events & Webinars:
carah.io/BaculaSystemsEvents



Discover Technology Solutions:
carah.io/BaculaSystemsSolutions



Learn About Procurement:
carah.io/BaculaSystemsContracts



Connect With Our Team:
BaculaSystems@carahsoft.com
571-590-4040

Post-VMware Protection

Backup Coverage Across the Six
Leading Migration Platforms

A Bacula Systems competitive whitepaper for enterprise architects, infrastructure leaders, and procurement teams evaluating their post-VMware data-protection strategy.

VERSION / DATE

Version 2.0 · May 2026

Table of Contents

Executive Summary..... 3

The Six Leading Migration Destinations..... 5

Coverage Matrix: Bacula vs. The Incumbents..... 12

Planning Data Protection for Your Migration..... 16

Commercial Model, Partners, and References.....19

Conclusion.....22



Executive Summary

The end of the perpetual VMware era is no longer a future scenario. Following Broadcom's acquisition of VMware and the subsequent restructuring of vSphere licensing, enterprises across every region and vertical are actively planning, piloting, or executing migrations away from vSphere. The Q1 2026 Vitrified Loop Survey found that 48% of VMware customers intend to reduce their VMware footprint by 2028, while 25% report that finding a suitable alternative is the single largest obstacle to that transition.

The market has responded. Ten vendors now meet Vitrified's enterprise inclusion criteria for hypervisor alternatives, and a clear top tier has emerged. For most enterprises, the migration target will be one — or, more often, several — of six platforms: Nutanix AHV, Microsoft Hyper-V and Azure Stack HCI, Red Hat OpenShift Virtualization, Proxmox VE, XCP-ng / KVM, and OpenStack.

Backup and data protection is rarely the headline workstream in a hypervisor migration, but it is one of the workstreams most likely to derail the timeline. Most incumbent backup platforms were architected around VMware vSphere; their support for the alternatives is uneven, partial, or — in the case of Proxmox and XCP-ng — entirely absent. Enterprises that fail to address protection coverage early in the migration discover the gap only after the cutover, when restore points stop, audits fail, or RPO commitments cannot be honored.



Executive Summary (continued)

This whitepaper provides a practical, vendor-comparative assessment of backup coverage across all six leading destinations. Section 2 profiles each platform and the migration patterns Bacula sees in the field. Section 3 presents a 41-row coverage matrix benchmarking Bacula Enterprise against Veeam v12, Commvault, Cohesity, and Rubrik.

Section 4 outlines a recommended engagement approach for accounts in active migration, and Section 5 closes with channel and commercial guidance for engaging through Kyndryl, Carahsoft, and the broader Bacula partner network.

Why this matters for backup architects

A single enterprise rarely consolidates onto one VMware alternative. Most organizations end up running two or three hypervisors in parallel for years — frequently Hyper-V for general-purpose workloads, OpenShift for containerized and net-new applications, and Proxmox or KVM for cost-sensitive or research environments.

If your data-protection platform supports only one or two of these, you will end up running multiple backup products. That fragmentation is a security risk, an operational burden, and a budget line item — and it is the single most common cost surprise in post-VMware programs.

The Six Leading Migration Destinations

The six platforms profiled below are the destinations Bacula encounters most frequently in active VMware migration accounts. They are not the only alternatives — Canonical LXD, Vates, and Scale Computing also appear in specific niches — but they account for the overwhelming majority of production cutover decisions in 2025–2026.

Nutanix AHV

Nutanix AHV is the most direct like-for-like replacement for VMware vSphere. For enterprises that want a turnkey hyperconverged platform with a single vendor delivering compute, storage, networking, and management, Nutanix is the path of least architectural disruption. Migration tooling is mature, partner ecosystems are deep, and the operational model is familiar to vSphere admins. AHV is built on a hardened KVM fork managed by the Nutanix Acropolis distributed storage fabric. Beyond core VM workloads, Nutanix Files (AFS) and Nutanix Objects extend the platform to file-share and S3-compatible object storage, both of which require independent backup coverage.

Architecture	Hardened KVM with Acropolis distributed storage fabric
Typical migrant	Mid-market and enterprise; existing Nutanix-on-ESXi customers; turnkey HCI buyers
Bacula coverage	AHV VMs, Nutanix Files (AFS), Nutanix Objects (S3); native Prism integration; changed-region tracking
Competitive note	All major incumbents support AHV VM backup; coverage depth for Files and Objects varies

Microsoft Hyper-V & Azure Stack HCI

For Microsoft-centric enterprises — particularly those with significant Azure consumption, existing System Center investment, or Windows Server Datacenter licensing already in place — Hyper-V and Azure Stack HCI represent the lowest incremental cost path off of VMware. Hyper-V ships with Windows Server at no additional licensing charge, and Azure Stack HCI extends the same hypervisor into a cloud-managed HCI configuration with consumption billing through the Azure portal.

Hyper-V's Resilient Change Tracking (RCT), introduced in Windows Server 2016 and matured in 2019/2022, provides VMware-equivalent incremental performance. Modern Hyper-V deployments increasingly run on Azure Stack HCI 22H2 or 23H2, where storage is provided by Storage Spaces Direct (S2D) and management has shifted to Azure Arc.

Architecture	Type-1 hypervisor on Windows Server; S2D storage on Azure Stack HCI variants
Typical migrant	Microsoft-aligned enterprises; existing Hyper-V shops repatriating from VMware; Azure-tiered deployments
Bacula coverage	Agentless backup via RCT; Cluster Shared Volume support; Azure Stack HCI 22H2/23H2 certified; Azure Blob tiering and archive
Competitive note	Strong incumbent coverage across the board; differentiation lies in licensing economics and air-gap architecture rather than feature presence

Red Hat OpenShift Virtualization

OpenShift Virtualization (OCP-V), based on the upstream KubeVirt project, allows traditional VMs and Kubernetes containers to coexist on a single OpenShift control plane. For enterprises already invested in OpenShift for cloud-native workloads — and for federal, intelligence, and defense customers running OpenShift in disconnected or air-gapped configurations — OCP-V is the strategic VMware alternative.

OCP-V's protection model is fundamentally different from a traditional hypervisor. VMs are Kubernetes custom resources; their disks are persistent volumes; cluster state lives in ETCD. A backup product that protects only the VM disk image and ignores ETCD, namespaces, and operator configurations cannot deliver a full disaster-recovery outcome.

Bacula's OpenShift Virtualization differentiation

Bacula Enterprise is the only platform in this comparison with full ETCD cluster-state backup, native operator-based deployment via the OpenShift Operator Lifecycle Manager (OLM), and validated support for disconnected (air-gapped) cluster recovery — the configuration required for IC, DoD, and classified national-security deployments.

Veeam's OpenShift Virtualization story is materially behind; Commvault, Cohesity, and Rubrik all support pieces of the stack but lack disconnected-cluster recovery validation.

Architecture	KubeVirt running on OpenShift Container Platform; VMs as Kubernetes custom resources
Typical migrant	Cloud-native-first enterprises; existing OpenShift customers; federal / IC / DoD with disconnected requirements
Bacula coverage	KubeVirt VMs, container workloads, persistent volumes, ETCD, namespaces, operators; disconnected-cluster validated
Competitive note	Bacula's strongest competitive position outside of Proxmox and XCP-ng; air-gap and ETCD coverage are unique to Bacula

Proxmox VE

Proxmox Virtual Environment is a mature, open-source hypervisor distribution built on Debian, KVM, and LXC. It has long been the dominant choice in cost-sensitive segments — small and mid-sized businesses, education, research labs, hosting providers — and the Broadcom-VMware transition has driven significant new adoption among enterprise accounts that would not have considered Proxmox three years ago. Proxmox Backup Server (PBS) extends the platform with a deduplicated backup repository optimized for Proxmox workloads.

Proxmox is where the gap between Bacula and the incumbents is widest. Of the four major incumbents, only Bacula provides native Proxmox VE backup. Veeam has zero Proxmox support today; Commvault, Cohesity, and Rubrik offer partial coverage limited to generic KVM agent paths that miss Proxmox-specific features such as LXC containers, PBS integration, and Ceph or ZFS backing-store awareness.

What Proxmox means for your backup strategy

If Proxmox is anywhere in your plans — even as a small footprint or pilot — its protection deserves early attention, because backup support for it varies widely. Veeam offers no Proxmox support today. Commvault, Cohesity, and Rubrik provide only partial coverage through generic-KVM workflows that do not match a production Proxmox deployment.

Bacula covers Proxmox VMs, LXC containers, PBS-integrated repositories, and Ceph and ZFS backing stores from a single console with cluster-aware scheduling.

Architecture	Debian-based KVM and LXC distribution with optional Ceph and ZFS storage; Proxmox Backup Server for native repository
Typical migrant	Cost-sensitive enterprises; SMB and mid-market; education and research; international markets; Broadcom-fatigued accounts
Bacula coverage	Native VM and LXC backup; PBS integration; Ceph and ZFS awareness; cluster-aware scheduling; full file-level recovery
Competitive note	Bacula is the only enterprise platform with full Proxmox coverage; Veeam has none

XCP-ng / KVM (libvirt)

XCP-ng is the open-source descendant of Citrix XenServer, and together with generic libvirt-managed KVM deployments it represents the pure open-source exit from VMware.

XCP-ng is most commonly paired with Xen Orchestra as a management plane and is gaining traction in European public sector, scientific computing, and sovereign-cloud accounts that cannot accept proprietary licensing dependencies.

Generic KVM via libvirt also underpins countless private-cloud and CloudStack deployments. (OpenStack, the largest libvirt-based private cloud and a major VMware-migration destination in its own right, is profiled separately in Section 1.6.) As with Proxmox, the major incumbents either do not support these environments at all or support them only via generic agent-in-guest paths that defeat the agentless operating model enterprises expect.

Architecture	XCP-ng (Xen-based) with Xen Orchestra; libvirt-managed KVM in OpenStack, CloudStack, or stand-alone
Typical migrant	European public sector; scientific computing and HPC; sovereign-cloud builders; CloudStack operators
Bacula coverage	XCP-ng with Xen Orchestra integration; generic libvirt / KVM with live-migration awareness; file-level recovery from images
Competitive note	Comprehensive XCP-ng coverage is a Bacula-only capability among the major incumbents

OpenStack

OpenStack is the open-source standard for full private-cloud infrastructure, and it has become one of the most significant beneficiaries of the VMware exodus — especially among telecommunications operators, sovereign-cloud builders, large service providers, and public-sector organizations that need a complete Infrastructure-as-a-Service platform rather than a standalone hypervisor. Where Proxmox and XCP-ng replace the vSphere hypervisor, OpenStack replaces the entire VMware Cloud Foundation stack: compute, block and object storage, software-defined networking, identity, and orchestration under one API-driven control plane.

The momentum is quantified. The OpenInfra Foundation reports that 82% of its members have fielded inquiries from organizations seeking a VMware alternative, and 61% have already migrated a VMware customer to an OpenStack-based platform. With more than 45 million cores in production worldwide and a steady six-month release cadence — the 2026.1 “Gazpacho” release being the most recent — OpenStack is a mature, enterprise-proven destination, not an emerging experiment.

OpenStack’s protection model spans several independent services, and a backup product must understand all of them. Nova governs compute instances; Cinder provides block volumes; Swift provides object storage; Neutron defines the software-defined network; Glance manages images; and Keystone enforces multi-tenant identity. A backup tool that captures only an instance’s boot disk — and ignores attached Cinder volumes, project and tenant boundaries, network topology, and image lineage — cannot deliver a usable recovery.

Bacula’s OpenStack differentiation

Bacula protects OpenStack through a dual-module architecture: a proxy-VM method that captures complete instances together with their Nova metadata, Neutron networking, Glance images, and attached Cinder volumes, plus a purpose-built Cinder backup driver for volume-level protection.

Combined with Swift object coverage, project- and tenant-aware scheduling, per-core licensing that does not penalize the dense core counts typical of OpenStack hosts, and CNSSI 4009-compliant air-gap for sovereign and disconnected deployments, Bacula is the natural fit for the telco and sovereign-cloud operators that dominate OpenStack adoption.

Veeam offers no native OpenStack backup; Cohesity and Rubrik fall back to generic KVM agent paths.

Architecture	Modular IaaS – Nova (KVM/libvirt compute), Cinder (block), Swift (object), Neutron (SDN), Glance (images), Keystone (identity)
Typical migrant	Telecommunications and service providers; sovereign-cloud and public-sector builders; large private-cloud operators; European and regulated markets
Bacula coverage	Proxy-VM instance backup (Nova/Neutron/Glance/Cinder); native Cinder backup driver; Swift object protection; project- and tenant-aware scheduling; agentless and agent-based options
Competitive note	Commvault offers comparable native coverage; Veeam has none; Cohesity and Rubrik rely on generic KVM agent paths

Coverage Matrix: Bacula vs. The Incumbents

The matrix benchmarks on the following pages pits Bacula Enterprise against the four most commonly displaced incumbent backup products — Veeam v12, Commvault, Cohesity, and Rubrik — across the six migration destinations and a final cross-platform section covering licensing, security, and architectural capabilities.

Status assessments are based on publicly documented support matrices, vendor reference architectures, certified-platform listings, and field validation as of Q1 2026.



✓ Full coverage	⦿ Partial / limited	✗ Not supported	— Not applicable
-----------------	---------------------	-----------------	------------------

Capability	Bacula	Veeam v12	Commvault	Cohesity	Rubrik
NUTANIX AHV					
Image-level VM backup via Prism API	✓	✓	✓	✓	✓
Changed-region tracking incrementals	✓	✓	✓	⦿	⦿
Application-consistent snapshots	✓	✓	✓	✓	⦿
Nutanix Files (AFS) protection	✓	⦿	✓	⦿	⦿
Nutanix Objects (S3) protection	✓	⦿	⦿	⦿	⦿
Mine-style appliance available	⦿	✓	⦿	✓	✓
MICROSOFT HYPER-V & AZURE STACK HCI					
Agentless Hyper-V backup via RCT	✓	✓	✓	✓	✓
Cluster Shared Volume (CSV) support	✓	✓	✓	✓	✓
Hyper-V 2022 (22H2/23H2) certified	✓	✓	✓	⦿	⦿
Azure Stack HCI native backup	✓	⦿	✓	⦿	⦿
Azure Blob tiering / archive	✓	✓	✓	✓	✓
SCVMM integration	✓	✓	✓	⦿	✗
RED HAT OPENSIFT VIRTUALIZATION (KubeVirt)					
KubeVirt VM-level backup	✓	⦿	✓	✓	✓
OpenShift container / pod protection	✓	⦿	✓	✓	✓
Persistent Volume (PV) snapshots	✓	⦿	✓	✓	✓
ETCD cluster-state backup	✓	✗	⦿	⦿	⦿

Capability	Bacula	Veeam v12	Commvault	Cohesity	Rubrik
Disconnected (air-gapped) cluster support	✓	✗	✗	✗	✗
Operator-based deployment (OLM)	✓	✗	◐	✓	✓
PROXMOX VE					
Proxmox VM (KVM) backup	✓	✗	◐	◐	◐
Proxmox LXC container backup	✓	✗	✗	✗	✗
Proxmox Backup Server integration	✓	✗	✗	✗	✗
Ceph backing-store awareness	✓	✗	✗	◐	◐
ZFS backing-store awareness	✓	✗	◐	◐	◐
Cluster-aware scheduling	✓	✗	✗	✗	✗
XCP-NG / KVM (libvirt)					
XCP-ng / Citrix Hypervisor backup	✓	✗	◐	✗	✗
Generic KVM / libvirt support	✓	✗	◐	◐	◐
Xen Orchestra integration	✓	✗	✗	✗	✗
VM live-migration awareness	✓	✗	◐	✗	✗
File-level recovery from KVM images	✓	✗	◐	◐	◐
OPENSTACK					
Nova instance-level backup (proxy method)	✓	✗	✓	◐	◐
Cinder volume protection (native driver)	✓	✗	✓	◐	✗
Swift object storage protection	✓	✗	◐	✗	✗
Project / tenant-aware backup	✓	✗	✓	✗	✗
Glance image & instance metadata	✓	✗	✓	◐	◐
Sovereign / disconnected OpenStack validated	✓	✗	◐	✗	✗



Capability	Bacula	Veeam v12	Commvault	Cohesity	Rubrik
CROSS-PLATFORM CAPABILITIES					
Per-core / per-socket licensing flexibility	✓	○	○	✗	✗
True air-gap (CNSSI 4009-compliant)	✓	○	○	○	○
FIPS 140-3 validated cryptography	✓	○	✓	○	○
Linux-native data mover	✓	✗	○	○	○
HPC / parallel-filesystem integration	✓	✗	○	✗	✗
Mainframe & AIX / Power coverage	✓	✗	✓	✗	✗

Status assessments are based on publicly documented support matrices, vendor reference architectures, certified-platform listings, and field validation as of Q1 2026. Where a vendor offers backup of a platform via a generic agent-in-guest mechanism that does not match the platform's native operating model, status is recorded as Partial.

Planning Data Protection for Your Migration

Most VMware migrations move through three stages, and the data-protection questions worth asking are different at each one.

Stage 1 — Strategy and platform selection

At this stage you are still evaluating which alternative — or combination of alternatives — to standardize on. Backup is rarely top of mind here, but it deserves a place in the discussion: data protection is the one workstream that must support every platform on your eventual target list, so protection coverage is worth weighing alongside the hypervisor decision itself.

- **Weigh protection breadth.** Choosing platform-neutral data protection keeps your hypervisor options open, so the decision is driven by your infrastructure needs rather than by a backup tool's limitations.
- **Account for open-source destinations.** If Proxmox, XCP-ng, or OpenStack are on your shortlist, confirm data-protection support early. Coverage for these platforms is uneven across incumbent backup products — Veeam supports none of the three natively — so any gap is best resolved before you commit.
- **Review protection architecture per platform.** Bacula's solution-architect team can work through a platform-by-platform protection design across your current and target environments during evaluation, so coverage is confirmed well before cutover.

Stage 2 — Pilot and parallel-run

You have selected a target hypervisor, stood up a pilot, and are running protected workloads on both vSphere and the new platform in parallel. This is where backup gaps tend to surface: limitations that were tolerable on vSphere become real problems once the same tool is pointed at the new platform.

- **Plan for parallel-protection costs.** Per-core licensing lets you extend protection to the new platform without re-licensing the entire estate; socket- or capacity-based models can require a full re-purchase during the parallel-run period.
- **Confirm air-gap and sovereignty requirements.** Migrations to disconnected OpenShift, sovereign-cloud KVM, or OpenStack environments often require a CNSSI 4009-compliant air-gap. Confirm that your backup platform can deliver it, as support varies across products.
- **Validate vendor claims against the matrix.** The coverage matrix in Section 2 turns a general 'we support that' assurance into a documented, line-by-line comparison you can check against each vendor's own support documentation.





Stage 3 — Production cutover and steady-state operations

You are running production workloads on the new platform and need a backup product that operates against it day-to-day. The priorities here are operational: console consolidation, automation maturity, and the ability to retire the legacy vSphere-only backup product.

- **Consolidate to a single console.** Bacula's single-console model across all six platforms eliminates the operational fragmentation that emerges from running one product for VMware, another for Proxmox, and a third for OpenShift.
- **Migrate the catalog, not just the workloads.** Bacula's catalog and retention model can ingest restore points and historical inventory from the displaced product, preserving compliance evidence across the cutover.
- **Consider managed-services and procurement options.** If you prefer managed delivery, Kyndryl operates Bacula as a managed service; for U.S. public sector, Carahsoft provides contract vehicles and channel routing. Both can shorten time-to-production.

Commercial Model, Partners, and References

Per-agent licensing flexibility

Bacula Enterprise is licensed per agent, with sizing based on the workload footprint rather than the storage capacity protected or the number of sockets in the source host. This matters in post-VMware migrations because the move itself often changes one or more of these underlying metrics in ways that penalize capacity- or socket-based competitors.

Customers consolidating onto Hyper-V or AHV typically run with denser core counts per host than they did on vSphere; capacity-based vendors charge for the resulting protected-data growth even when the underlying business workload has not changed. Customers moving to OpenShift, Proxmox, or XCP-ng often see large changes in the storage layer (Ceph, ODF, S2D) that can re-bracket their license tier with no policy change. Bacula's per-core model removes both of these surprises.

The Carahsoft partnership and U.S. public sector

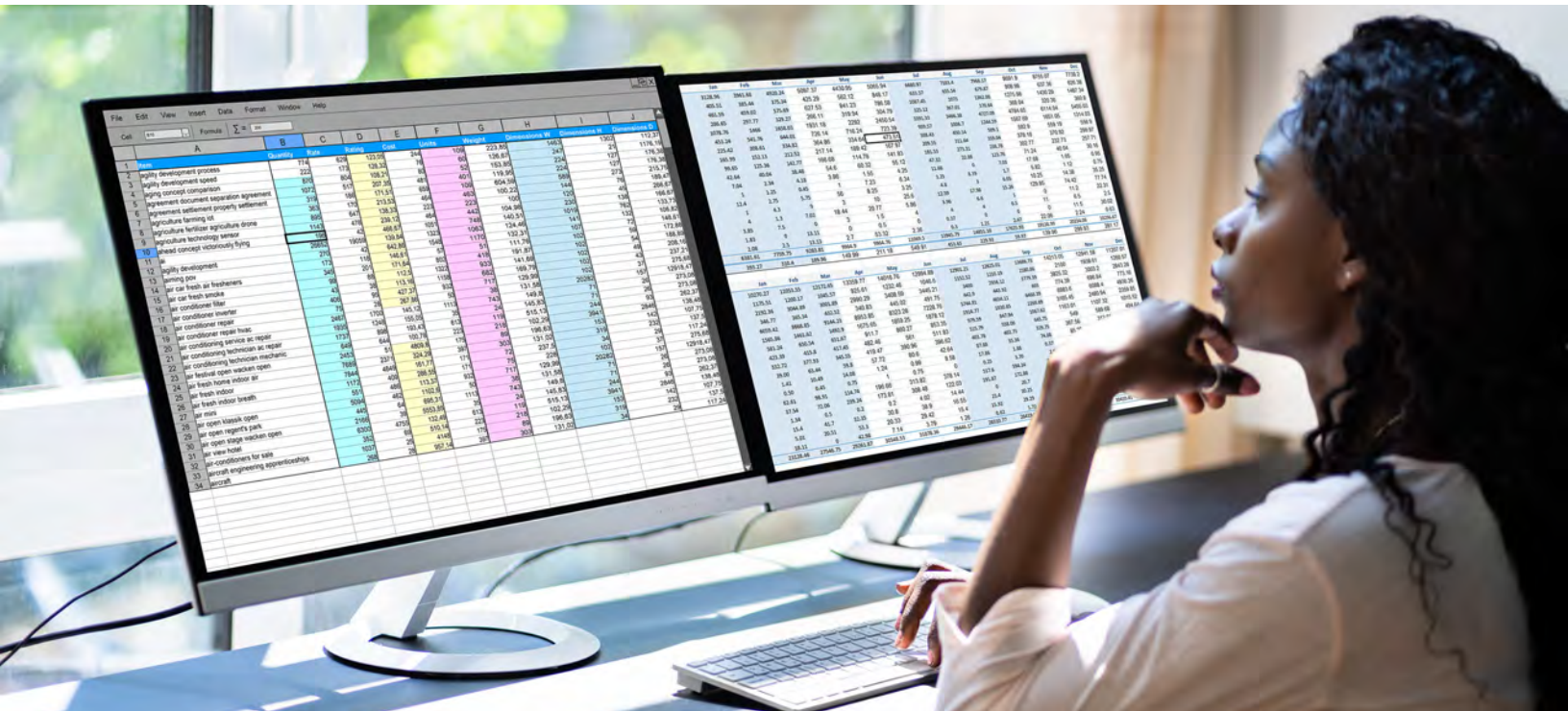
For U.S. federal, defense, intelligence community, and SLED accounts, Bacula is available through Carahsoft and the Bacula microsite at carahsoft.com/bacula-systems, with the Carahsoft sales team reachable at BaculaSystems@carahsoft.com. Carahsoft provides aggregated contract vehicle access, channel partner routing, and U.S. public sector compliance enablement.

Carahsoft is particularly relevant for OpenShift and KVM migrations in the federal space, where disconnected-cluster requirements, FIPS validation, and CNSSI 4009 air-gap compliance are mandatory.

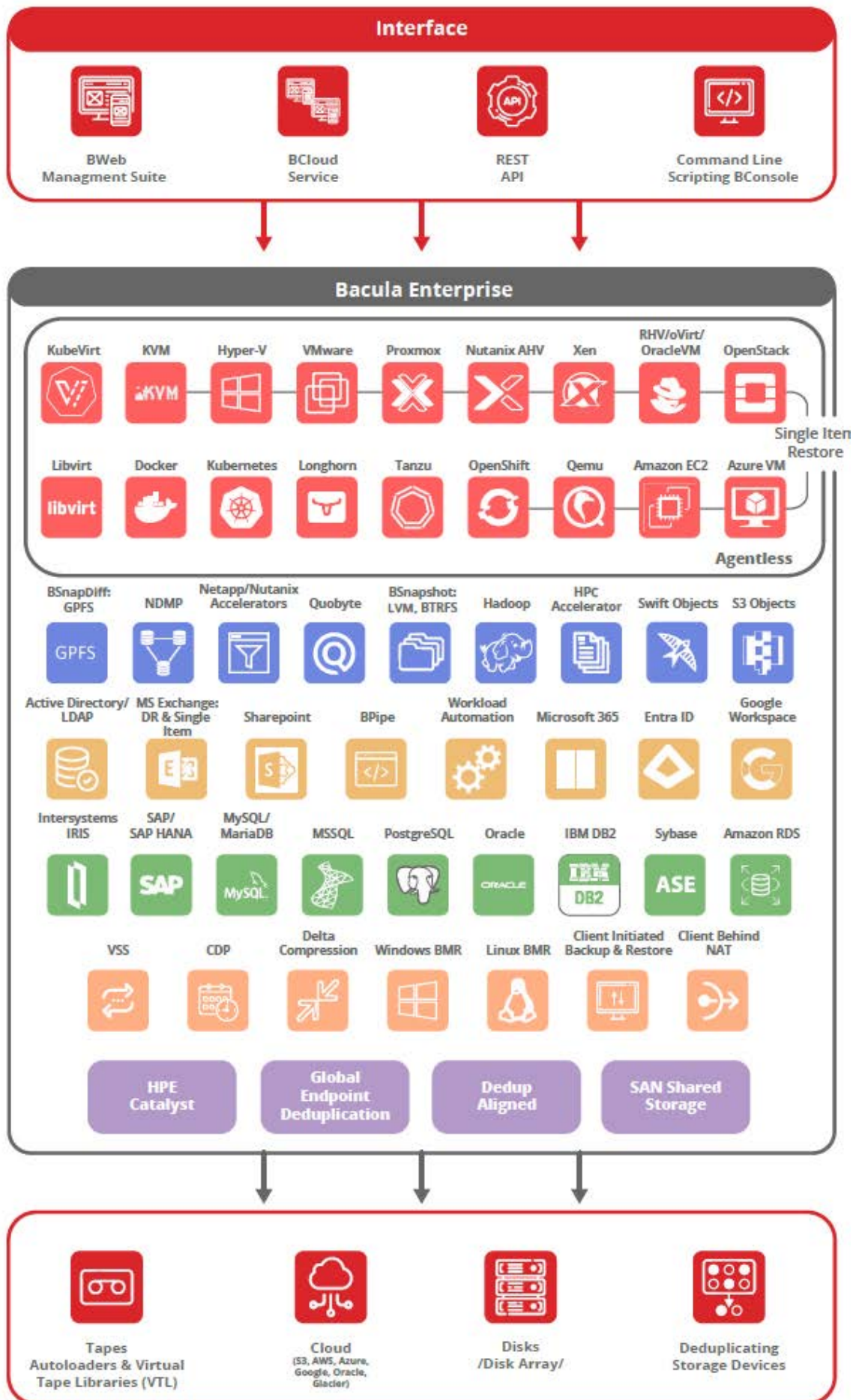
Bacula's compliance whitepaper portfolio on the Carahsoft microsite — covering CMMC 2.0, Zero Trust IC, CJIS, FedRAMP/FISMA, StateRAMP, DOE Order 205.1D, and GovCloud — provides the documentation a federal procurement officer needs to validate Bacula's place on the shortlist.

Proven-at-scale references

Bacula's reference deployments demonstrate operation at the scale post-VMware enterprises require: Los Alamos National Laboratory, Idaho National Laboratory, Sandia, NASA, Booking.com, Deutsche Bahn, and Options Technology among them. These references span every architecture profile in this whitepaper, from sovereign-cloud KVM to disconnected OpenShift to converged Hyper-V to large-scale Nutanix AHV.



Bacula Enterprise natively integrates with more technologies than any other data protection vendor



Conclusion

The post-VMware market is no longer a single-platform decision. Most enterprises will end up running two, three, or four hypervisors in parallel for the foreseeable future, and the data-protection product that supports that mix is the one that earns the long-term position in the account.

Across the six leading migration destinations — Nutanix AHV, Microsoft Hyper-V and Azure Stack HCI, Red Hat OpenShift Virtualization, Proxmox VE, XCP-ng / KVM, and OpenStack — Bacula Enterprise is the only platform in this comparison with full coverage of all six. That breadth is reinforced by per-core licensing flexibility, CNSSI 4009-compliant air-gap, FIPS 140-3 cryptography, Linux-native architecture, and HPC-grade scalability.

Combined with the Kyndryl managed-services partnership, the Carahsoft public sector channel, and a reference base that includes the world's most demanding research, transportation, financial, and national-security workloads, Bacula is positioned to be the data-protection foundation underneath every post-VMware destination an enterprise chooses.

Next steps

Engage your Bacula account team for a platform-by-platform protection-architecture review against your current and target hypervisor estate.

U.S. public sector accounts: contact the Carahsoft team at BaculaSystems@carahsoft.com or visit carahsoft.com/bacula-systems.

Enterprise accounts seeking managed-services delivery: request a joint engagement with Kyndryl through your Bacula account team.

Final Insight: Bacula Enterprise offers significantly higher levels of security than its peers. In-depth training and materials are available for IT professionals that require further, deeper and more granular information on Bacula Enterprise's unique security profile.

Start now to protect your data today, and for the decades ahead. Contact Bacula Systems for a tailored backup and recovery security consultation at **sales@baculasystems.com**



About Bacula Systems

Bacula Systems is an enterprise backup software company serving the U.S. Intelligence Community through Carahsoft Technology Corp. as authorized public sector partner. Bacula's existing IC-component deployments at Los Alamos National Laboratory, Idaho National Laboratory, and Sandia National Laboratories provide established credibility under the new ODNI ATO reciprocity framework.

www.baculasystems.com · Carahsoft microsite: carahsoft.com/bacula-systems

Competitive capability assessments are based on publicly available documentation and independent research. Bacula Systems SA reserves the right to update this document as market conditions evolve.