Beyond VMware:

A RUBRIK VIEW OF HYPERVISORS

Document - reviewed against public sources on May 8, 2026

Working headline: Make hypervisor diversification a recoverability decision, not only a licensing decision.

Editorial note for publication: The statement that HPE Morpheus VM Essentials / HVM will become a native Rubrik backup and restore target later in 2026 is treated in this draft as a roadmap item supplied by the requester. Public HPE and Morpheus documentation currently shows VM Essentials backup capabilities and Rubrik integration for vCenter cloud backup management, but I did not find a public Rubrik GA announcement for native HVM backup target support. Confirm exact wording, dates, feature scope, and safe-harbor language with Rubrik product management before external publication.

Audience: CIOs, infrastructure leaders, virtualization architects, backup and recovery owners, and partners helping customers evaluate VMware alternatives.

SEO focus: VMware alternatives, Rubrik backup for Hyper-V, Rubrik Nutanix AHV, Rubrik Proxmox, Rubrik OpenShift Virtualization, Rubrik OLVM, HPE Morpheus VM Essentials, Cristie RBMR, bare metal recovery.

EXECUTIVE SUMMARY

Broadcom completed its acquisition of VMware on November 22, 2023. Since then, many enterprise infrastructure teams have re-opened the hypervisor decision. Cost, licensing, support models, and strategic vendor concentration are part of the discussion, but they are not the whole discussion. A hypervisor migration that is not recoverable is not a modernization plan; it is a new risk surface. [1]

The practical question is not simply "Which hypervisor can replace VMware?" The better question is: "Which target platform can we protect, recover, test, and operate with the same confidence we expect from our current Rubrik-protected estate?" Recent market research illustrates why this matters: CloudBolt reported in February 2026 that 86 percent of surveyed North American enterprise IT decision-makers were actively reducing their VMware footprint, with 88 percent expressing concern about future price increases. [2]

Rubrik gives customers a path to make that decision workload by workload. Where Rubrik has native hypervisor integrations, customers can preserve policy-driven protection, immutable backups, and streamlined recovery workflows. Where a hypervisor is not natively supported, Rubrik Backup Service (RBS) can still protect the operating system, file system, and application data from inside the guest. For disaster recovery and bare machine recovery across unsupported or non-native targets, Cristie RBMR can recover systems directly from Rubrik Security Cloud backups and help rebuild into physical, virtual, or cloud targets. [9][14]

This blog looks at the main VMware alternatives through a Rubrik lens: what is supported, what is practical, and what limitations must be designed around before migration.

Key takeaways

- **Do not treat all hypervisors as equal from a backup perspective**. The operational difference is not the hypervisor logo; it is whether Rubrik can discover the VM, snapshot it, index it, recover it, and preserve the metadata needed for fast restore.
- **Use native Rubrik integrations where available**. Public Rubrik material now describes native or purpose-built coverage for Microsoft Hyper-V, Azure Local / Azure Stack HCI, Nutanix AHV, Red Hat OpenShift Virtualization, Proxmox VE, and Oracle Linux Virtualization Manager (OLVM), with vSphere remaining the baseline for many estates. [4][6][7][10][11][12]
- **Assume feature parity must be proven, not inferred.** The fact that a platform is supported does not mean every VMware recovery operation behaves identically. Validate Live Mount, Instant Recovery, Export, guest file recovery, in-place recovery, archive/replica recovery, app consistency, and scale limits for each platform.
- **Keep an agent-based pattern for edge cases.** RBS protects guest operating systems, file systems, and application data when the hypervisor itself has no native Rubrik integration. Cristie RBMR can add bare machine recovery and dissimilar-target recovery for DR scenarios. [9][14]
- **Treat HPE Morpheus VM Essentials as a near-term roadmap decision.** HPE positions VM Essentials as a KVM-based alternative with HVM hypervisor capabilities. Native Rubrik backup/restore support for HVM should be piloted after Rubrik publishes the supported versions and feature scope. [13]

RUBRIK VIEW OF ALTERNATIVE HYPERVISORS

The table below is written for planning purposes. Always verify against the current Rubrik Compatibility Matrix, because Rubrik explicitly limits support to configurations and integrations specified in its compatibility documentation. [3]

Platform	Rubrik posture	Primary protection model	Recovery capabilities to validate
Microsoft Hyper-V	Native Rubrik support. Public compatibility material includes Hyper-V 2016, 2019, 2022, and 2025; SCVMM is optional depending on design. [4]	Rubrik manages Hyper-V through Microsoft APIs; Hyper-V protection uses Resilient Change Tracking. RBS is required on Hyper-V hosts and optional inside guests. [5][9]	Instant Recovery, Live Mount, Export, mount virtual disks, and download VM-level files; replica-based recovery cannot use some actions. [5]
Azure Local / Azure Stack HCI	Supported as Hyper-V protected objects in Rubrik CDM for listed Azure Local releases. [6]	Hyper-V-style protection for Azure Local clusters.	Treat it as a validated Hyper-V/Azure Local design, not as generic Azure VM protection. Rubrik documentation notes that Azure Local does not support Filesets and Windows Volume Groups. [6]
Nutanix AHV	Native Rubrik support across many AOS releases. [7]	Agentless AHV VM protection through Nutanix integration; RBS in the guest can be used for VSS/app-aware needs. [7][9]	Recover files, Live Mount, Export, mount/download virtual disks, in-place recovery, and Instant Recovery; recoveries require locally available snapshots. Exported disks use SCSI and CD-ROM drives use IDE, which can affect bootability. [7][8]
Red Hat OpenShift Virtualization	Rubrik protection for OpenShift containers and VMs is publicly described in Rubrik solution and documentation pages. [10]	Kubernetes/OpenShift-oriented protection model; VMs are discovered in RSC and protected with SLA Domains.	Validate storage class behavior, cluster-to-Rubrik mapping, protection-set granularity, VM-level recovery, and capacity impact. [10]
Proxmox VE	Rubrik announced Rubrik for Proxmox VE as generally available on April 21, 2026. [11]	Native Proxmox API discovery, policy-driven protection, immutable backup storage, and Proxmox-focused recovery workflows. [11]	Public launch material emphasizes full VM restore/export recovery and global search. Validate whether your required feature set includes Live Mount, in-place recovery, guest file recovery, or app-consistency mechanisms. [11]
Oracle Linux Virtualization Manager (OLVM)	Rubrik announced OLVM support as generally available in January 2026. [12]	Onboard oVirt Engine, auto-discover VMs, apply SLA Domains, take an initial full image backup, then incremental backups. [12]	Public solution material lists LiveMount, Export, and Files/Folders recovery; validate exact version support, feature parity, and application consistency. [12]
HPE Morpheus VM Essentials / HVM	Roadmap in this draft: native Rubrik backup/restore target support later in 2026; public GA statement not found. HPE currently describes VM Essentials as including the HVM hypervisor. [13]	Until native Rubrik support is GA, use RBS in guests for OS/file/app data and use Cristie RBMR for bare machine recovery to HVM where appropriate. [9][14]	Confirm Rubrik-supported HVM versions, discovery model, snapshot model, Live Mount/Export behavior, file recovery, app consistency, scale limits, and safe-harbor language before publishing.
Other KVM/Xen/edge hypervisors	No native Rubrik hypervisor integration should be assumed unless the Rubrik Compatibility Matrix explicitly lists it. [3]	Guest-level RBS protection, Rubrik application protection, file sets, and/or managed volume patterns, depending on workload.	No native VM inventory, SLA inheritance, hypervisor snapshot orchestration, instant mount, or VM metadata restore. Add RBMR for DR and dissimilar-target recovery. [9][14]

NATIVE INTEGRATION VERSUS GUEST-LEVEL PROTECTION

The cleanest migration outcome is native Rubrik integration on the target hypervisor. Native integration gives Rubrik a control-plane relationship with the virtualization platform: discovery, SLA assignment, snapshot orchestration, metadata awareness, and recovery actions that can recreate VMs or expose their disks and files. That is why native support should be the first design option for mainstream replacement platforms.

But native hypervisor integration is not the only way to preserve recoverability. RBS can be installed in supported operating systems to coordinate protection and recovery between the workload and Rubrik. Public Rubrik documentation describes RBS as a prerequisite for protecting several workload types, including physical systems, Hyper-V hosts, databases, Windows volume protection, and VM quiescing or file recovery workflows. [9]

The trade-off is control-plane visibility. With RBS alone, Rubrik sees and protects the guest workload, not necessarily the surrounding hypervisor object. It can recover files, volumes, and application data according to the protected workload type, but it does not automatically recreate every VM setting, network mapping, boot firmware setting, virtual hardware attribute, affinity rule, or hypervisor-specific policy. That is where a DR tool such as Cristie RBMR becomes important.

Cristie RBMR for Rubrik is positioned to recover systems directly from Rubrik Security Cloud backups, run DR simulations, and recover across physical, virtual, and cloud targets. [14] For unsupported hypervisors, that makes RBS plus RBMR the practical fallback pattern: protect the OS, data, and applications inside the guest; test full-system recovery into the target hypervisor; and document the manual or automated steps needed to recreate the VM wrapper.

Design principle

Use native Rubrik integrations for production-scale hypervisor migrations whenever possible. Use RBS plus Cristie RBMR for unsupported platforms, edge cases, and DR portability - but treat it as a different operating model with different RTO, automation, and test requirements.

PLATFORM BY PLATFORM GUIDANCE

Microsoft Hyper-V

Rubrik posture: Native Rubrik support for listed Hyper-V releases. Rubrik public compatibility material includes Hyper-V Server / Windows Server Hyper-V 2016, 2019, 2022, and 2025, and corresponding SCVMM releases where used. [4]

Best-fit use case: Organizations standardizing on Microsoft virtualization, especially where Windows Server, Active Directory, SQL Server, and System Center skills are already strong.

Protection model: Rubrik manages Hyper-V through Microsoft APIs and uses Resilient Change Tracking for forever-incremental protection. RBS is required on the Hyper-V host; guest RBS is optional and useful for guest-level workflows and application consistency. [5][9]

Recovery model: Rubrik documentation lists Instant Recovery, Live Mount, Export, mount virtual disks, and download VM-level files for Hyper-V VM recovery. [5]

Limitations and design checks:

- **Replica restrictions:** Rubrik documentation states that recovery using a replica cannot use Instant Recovery, Mount Virtual Disks, or Download VM Files. Plan replica-based DR accordingly. [5]
- **Host prerequisites:** The Rubrik matrix notes language pack and version requirements; validate host, SCVMM, and cluster configuration before migration. [4]
- **Application consistency:** Use guest-aware protection and supported application integrations where crash-consistent VM recovery is not sufficient.
- **Operational difference from vSphere:** Do not assume vSphere runbooks translate one-to-one. Rebuild recovery playbooks for Hyper-V naming, networking, cluster CSV layout, and failover behavior.

Azure Local / Azure Stack HCI

Rubrik posture: Rubrik public compatibility material identifies Azure Local support through Hyper-V protected objects for listed Azure Local releases. [6]

Best-fit use case: Customers who want a Microsoft-aligned, on-premises hyperconverged platform with Azure management adjacency.

Protection model: Treat Azure Local as a specialized Hyper-V design: Rubrik protects the Hyper-V VM objects on the Azure Local cluster rather than treating them like native Azure cloud VMs. [6]

Recovery model: Recovery behaviour follows the supported Hyper-V/Azure Local object model and should be validated per release and cluster design.

Limitations and design checks:

- **Unsupported object types:** Rubrik compatibility information notes that Azure Local does not support Filesets and Windows Volume Groups. Use other supported methods for those workloads. [6]
- **Version sensitivity:** Azure Local is a fast-moving platform. Validate CDM/RSC, Azure Local release, Windows Server build, storage, and cluster configuration together.
- **Storage and network runbooks:** Recovery time depends on cluster capacity, storage path, and network mappings. Test restore under degraded cluster conditions, not only in a healthy lab.

Nutanix AHV

Rubrik posture: Native Rubrik support across many Nutanix AOS releases, with Prism Central support constraints documented in the Rubrik matrix. [7]

Best-fit use case: Enterprises that want an integrated HCI stack and a mature non-VMware virtualization target.

Protection model: Rubrik integrates with Nutanix AHV for VM protection and recovery. For Windows VMs and workloads needing application-consistent protection, Rubrik documentation points to RBS installation for VSS-consistent backups. [7][9]

Recovery model: Rubrik documentation describes file recovery, Live Mount, Export, mount virtual disks, download virtual disks, in-place recovery, and Instant Recovery for AHV VMs. [7]

Limitations and design checks:

- **Local snapshot requirement:** Rubrik documentation indicates AHV recovery can be performed from locally available snapshots, and not from snapshots that exist only in remote archives or replica targets. Design archive and replication flows with that constraint in mind. [7]
- **Export bus behavior:** Rubrik documentation notes that AHV export operations always export VM disks as SCSI and CD-ROM drives as IDE; if the guest OS cannot boot with those bus types, an exported VM can fail to boot. This limitation does not apply to Live Mount. [8]
- **Prism Central dependency:** The Rubrik matrix includes conditions for Prism Central support; validate Prism Central placement and AOS patch levels. [7]
- **App recovery:** For databases and application workloads, protect the application explicitly rather than relying only on image-level crash consistency.

Red Hat OpenShift Virtualization

Rubrik posture: Rubrik publicly describes cyber-resilient VM migration, backup, and recovery for Red Hat OpenShift Virtualization, with RSC discovering OpenShift VMs and applying SLA Domains. [10]

Best-fit use case: Organizations moving toward Kubernetes-native operations while still needing to run traditional VM workloads.

Protection model: OpenShift Virtualization protection follows the Kubernetes/OpenShift model. Public Rubrik material describes automated VM discovery, policy-driven backups, and recovery of VMs, containers, or individual files. [10]

Recovery model: Recovery should be planned around OpenShift resources, persistent volumes, namespaces, and storage classes rather than classic hypervisor-only semantics.

Limitations and design checks:

- **Different recovery semantics:** A VM in OpenShift Virtualization is a Kubernetes-managed workload. Validate namespace, PVC/PV, storage class, CDI/Data Volume, and network attachment behavior during restore.
- **Cluster association:** Rubrik documentation notes limitations around OpenShift cluster connection to Rubrik CDM and VM recovery from protection set snapshots. Protect workloads at the right granularity for the restores you need. [10]
- **Capacity planning:** VM backup volume can be substantial in container platforms. Validate Rubrik cluster capacity and storage snapshot behavior before broad rollout. [10]
- **Operational ownership:** Backup teams and platform teams must jointly own restore tests because the restore involves Kubernetes constructs as well as VM data.

Proxmox VE

Rubrik posture: Rubrik announced Rubrik for Proxmox VE as generally available on April 21, 2026. [11]

Best-fit use case: Cost-conscious organizations standardizing on an open-source virtualization platform, especially where Linux/KVM skills are strong and VMware dependency reduction is a near-term priority.

Protection model: Rubrik public material describes direct Proxmox API integration, automated discovery, SLA-driven protection, immutable backup storage, and recovery directly to Proxmox environments. [11]

Recovery model: Rubrik launch material emphasizes full VM restore/export recovery, search, and direct recovery into Proxmox. [11]

Limitations and design checks:

- **Feature parity must be validated:** Public GA material does not, by itself, prove parity with mature vSphere workflows. Validate Live Mount, in-place recovery, granular file recovery, guest indexing, application consistency, archive restore, and replica restore against current RSC documentation.
- **Hypervisor agent model:** Public Rubrik material describes a backup agent installed on the hypervisor to extract frozen VM disk data. Design upgrade, security, and change-control processes around that component. [11]

- **Operational maturity:** Proxmox adoption can move quickly because of cost pressure, but production recoverability requires standard VM templates, storage policies, network naming, and tested restore runbooks.
- **Fallback design:** Use RBS and RBMR for workloads where native Proxmox protection does not yet meet application, bare machine, or DR portability requirements. [9][14]

Oracle Linux Virtualization Manager (OLVM)

Rubrik posture: Rubrik announced generally available support for Oracle Linux Virtualization Manager in January 2026. [12]

Best-fit use case: Oracle-centric estates, Linux/KVM-oriented infrastructure teams, and customers looking for a supported enterprise virtualization stack outside VMware.

Protection model: Rubrik public solution material describes onboarding the oVirt Engine, automatically discovering VMs, applying inherited SLAs, taking an initial full image backup, and then high-speed incremental backups. [12]

Recovery model: Public Rubrik material lists LiveMount, Export, and Files/Folders recovery options for OLVM. [12]

Limitations and design checks:

- **Initial full backup:** Plan capacity and network load for the first full image backup before incremental steady state. [12]
- **Scale design:** Rubrik public material references a design point of up to 5,000 VMs; validate whether your inventory, churn rate, and SLA mix fit that envelope. [12]
- **Feature scope:** Do not infer VMware parity. Validate in-place recovery, instant recovery, cross-cluster export, archive retrieval, and file-level restore behavior for your exact OLVM release.
- **Application consistency:** Use RBS or Rubrik application integrations for Oracle Database and other applications where image-level restore alone is insufficient. [9]

HPE Morpheus VM Essentials / HVM

Rubrik posture: HPE positions VM Essentials as a virtualization solution that includes the HVM hypervisor and can manage VM Essentials and VMware vSphere virtual machines. This draft treats native Rubrik HVM backup/restore target support as a planned later-2026 roadmap item that must be confirmed before publication. [13]

Best-fit use case: Customers who want a managed KVM-based vSphere alternative with HPE enterprise packaging, HPE operational support, and a path to reduce VMware footprint while keeping familiar VM provisioning workflows.

Protection model: Until native Rubrik support is generally available and documented, protect workloads inside the guest with RBS and use Rubrik application protection where applicable. Use Cristie RBMR for full-system recovery and DR portability into HVM. [9][14]

Recovery model: Native Rubrik recovery scope should be piloted after GA. Before GA, recovery is guest-centric: file, volume, application, and full-system recovery via RBMR rather than Rubrik-native hypervisor reconstruction.

Limitations and design checks:

- **Public documentation gap:** HPE public documentation shows VM Essentials built-in backup/restore and a Rubrik Backup integration for vCenter Clouds in HPE Morpheus Enterprise, but that is not the same as a public Rubrik GA statement for native HVM backup target support. [13]
- **Roadmap language:** Use safe-harbor wording until Rubrik publishes exact supported versions, feature scope, and GA timing.
- **Pre-GA design:** For critical workloads, install RBS in supported guest operating systems, protect application data explicitly, and test Cristie RBMR recovery into HVM templates with the right VirtIO/storage/network drivers. [9][14]
- **HVM platform specifics:** HPE documentation describes VM Essentials as including HVM and supporting VM backup/restore, live migration, HA, external storage integrations, and synthetic full backup options. Validate storage and network prerequisites for backup/recovery performance. [13]

UNSUPPORTED OR NOT-YET-NATIVE HYPERVISORS

Rubrik posture: No Rubrik native hypervisor support should be assumed unless the current Rubrik Compatibility Matrix explicitly lists the hypervisor and version. [3]

Best-fit use case: Edge platforms, regional platforms, lab platforms, service-provider platforms, generic KVM, Xen-based platforms, or early-stage VMware alternatives where native Rubrik integration is absent.

Protection model: Use RBS inside supported guest operating systems. Depending on the workload, protect file systems, Windows volumes, Linux file sets, databases, or application data. Use Rubrik application integrations wherever they are a better fit than file-only protection. [9]

Recovery model: Restore to a manually provisioned VM, recover files/applications/volumes, or use Cristie RBMR to rebuild the system onto a new VM, physical server, or cloud target. [14]

Limitations and design checks:

- **No hypervisor inventory:** Rubrik will not automatically discover and classify VMs from the unsupported hypervisor.
- **No native hypervisor snapshot orchestration:** Guest-level protection does not replace hypervisor-aware snapshots for every workload. Quiescence, crash consistency, and application consistency must be designed.
- **No automatic VM metadata recreation:** Guest-level restore will not automatically recreate CPU, memory, firmware, disk controller, NIC, VLAN, MAC address, affinity, or placement metadata.
- **RTO impact:** Recovery may require creating a new VM shell, attaching storage, booting RBMR media, injecting drivers, restoring system state, and validating networking before application recovery.
- **Test obligation:** Run scheduled recovery simulations. Unsupported-hypervisor recovery is only credible when it has been executed, timed, and documented.

The RBS plus Cristie RECOVERY ASSURANCE & RBMR pattern for unsupported hypervisors

When a chosen hypervisor is not natively supported by Rubrik, the design target changes. You are no longer designing an agentless VM backup architecture. You are designing a guest-aware data protection and system recovery architecture. That can still be robust, but the responsibilities are different.

1. **Install RBS in the guest where supported.** Validate the guest OS against Rubrik-supported RBS platforms, including Windows, Linux, AIX, Solaris, and HP-UX variants where applicable. [9]
2. **Protect the workload at the right layer.** File sets are enough for some servers; Windows Volume Groups, database protection, or application-native Rubrik integrations may be required for others.
3. **Create a target VM template.** For each unsupported hypervisor, maintain golden VM templates with correct firmware mode, disk controller, NIC driver, storage path, and boot configuration.
4. **Use Cristie RBMR for full-system recovery.** RBMR can recover from Rubrik Security Cloud backups and automate or simulate recovery across physical, virtual, and cloud targets. [14]
5. **Document manual hypervisor steps.** Capture CPU/memory sizing, disk layout, network mappings, static routes, DNS, service accounts, IPAM updates, and post-restore application checks.
6. **Run clean-room restore tests.** A written design is not evidence. A time-stamped recovery test, including boot validation and application validation, is evidence.

A recoverability-first migration playbook

Hypervisor diversification should be staged. The goal is not to move the most VMs the fastest; it is to move the right workloads to the right platform without weakening recovery assurance.

Phase	What to do	Rubrik-specific checks
1. Inventory	Classify every VM by business service, OS, application, data size, change rate, dependencies, RTO, RPO, compliance retention, and restore granularity.	Confirm whether each workload is protected today by image-level VM backup, guest-level RBS, application protection, NAS, database, or another Rubrik object.
2. Segment	Group workloads into native-target candidates, RBS/RBMR candidates, application-level-only candidates, and workloads that should remain on VMware for now.	Do not migrate workloads that require recovery actions unavailable on the target platform until the gap is accepted or mitigated.
3. Pilot native platforms	Run pilots for Hyper-V, AHV, OpenShift Virtualization, Proxmox, OLVM, or HPE VM Essentials when native support is available.	Test backup, SLA assignment, archive, replica, file recovery, Live Mount/Instant Recovery/Export as applicable, and application consistency.
4. Build unsupported runbooks	For non-native hypervisors, build RBS plus RBMR recovery procedures and target VM templates.	Measure the real RTO and document every manual step. Use those results in platform selection, not just cost models.
5. Migrate in waves	Move low-risk workloads first, then progressively more critical services. Keep source-side Rubrik backups through the validation period.	Do not expire source backups until the target platform has passed restore tests and recovery owners sign off.
6. Operationalize	Update monitoring, patching, identity, RBAC, DR tests, retention, archive, cyber recovery, and escalation paths.	Make Rubrik SLA Domains, reporting, anomaly monitoring, and recovery testing part of the new hypervisor operating model.

Decision tree: choosing the right Rubrik protection path

1. **Is the target hypervisor listed in the current Rubrik Compatibility Matrix for the versions you will run?** Use the native integration path. If not, use RBS/RBMR or choose a different target.
2. **Does the workload require fast VM-level recovery such as Live Mount, Instant Recovery, or direct export?** Validate the exact action on the target hypervisor. Support for backup does not automatically imply every recovery action.
3. **Does the workload require application-consistent restore?** Add RBS or Rubrik application protection where image-level protection is not enough.
4. **Will backups live in archive or replication targets at the time of recovery?** Validate restore behavior from local snapshots, remote archives, and replicas. AHV and Hyper-V documentation show that recovery source can affect available actions. [5][7]
5. **Is the target HPE Morpheus VM Essentials / HVM before native Rubrik GA?** Use RBS plus Cristie RBMR and clearly separate that interim pattern from the planned native integration. [9][14]
6. **Is recovery the reason for the migration, not just a requirement of it?** Use clean-room recovery, RBMR simulations, and Rubrik reporting to prove that the new platform is recoverable under real operating assumptions.

Suggested Rubrik customer messaging

Rubrik customers do not need to make the VMware decision in a vacuum. A hypervisor evaluation should include a recoverability matrix alongside the cost and operations matrix. The platforms most attractive commercially may not be the best first targets for tier-1 workloads if recovery operations are immature, unsupported, or untested.

- **For VMware estates staying on vSphere:** Continue to use Rubrik to strengthen cyber resilience, reduce recovery uncertainty, and prepare for phased workload mobility.
- **For supported alternatives:** Use native Rubrik integrations to preserve policy-driven protection and test the target-specific recovery actions before migration waves.
- **For HPE Morpheus VM Essentials:** Position the platform as a strategic option but align public messaging to Rubrik roadmap/GA guidance. Until native support is available, protect with RBS and recover full systems with Cristie RBMR where required.
- **For unsupported hypervisors:** Do not overstate automation. RBS plus RBMR can protect and recover the workload, but the team must own VM shell recreation, driver compatibility, target networking, and DR tests.

BOOK A MASTER CLASS

Contact Cristie to book your Master Class today. www.cristienordic.com

Sources checked

Public sources checked on May 8, 2026. Required partner status.

[1] Broadcom, "Broadcom Completes Acquisition of VMware," November 22, 2023. Source link

[2] CloudBolt Software, "New CloudBolt Research: 86% of Companies Actively Reducing their VMware Footprint," February 17, 2026. Source link

[3] Rubrik Compatibility Matrix, document scope and support statement. Source link

[4] Rubrik Compatibility Matrix, Hyper-V virtualization environments. Source link

[5] Rubrik documentation, Hyper-V virtual machine recovery and Hyper-V protection model. Source link

[6] Rubrik Compatibility Matrix, Azure Local / Azure Stack HCI support notes. Source link

[7] Rubrik Compatibility Matrix and documentation, Nutanix AHV virtualization and AHV VM recovery. Source link

[8] Rubrik documentation, Nutanix export limitations for AHV VM disks and CD-ROM drives. Source link

[9] Rubrik documentation, Rubrik Backup Service and supported host operating systems. Source link

[10] Rubrik solution and documentation pages for Red Hat OpenShift Virtualization protection. Source link

[11] Rubrik, "Rubrik for Proxmox VE: Secure Proxmox Backups are Now Generally Available," April 21, 2026, and Rubrik Proxmox solution page. Source link

[12] Rubrik, "Rubrik Support for Oracle Linux Virtualization Manager: Safeguard Workloads, Enhance Resilience," January 21, 2026, and Rubrik OLVM solution page. Source link

[13] HPE Morpheus VM Essentials product and documentation pages; HPE Morpheus Rubrik backup integration documentation. Source link

[14] Cristie Software, RBMR for Rubrik and Cristie/Rubrik partnership pages. Source link