How businesses can protect and migrate workloads across and between physical servers, hypervisors and cloud platforms

Introduction

Every business needs a backup tool that is flexible enough to protect all of its physical, virtual and cloud platforms, and to enable fast, safe recovery of any workload to the same platform, to a new bare-metal server, to a different hypervisor platform or to the cloud as needed. That freedom of movement can provide protection against common IT challenges, e.g., a tech vendor that no longer meets the organization's needs.

Hypervisor vendor VMware provides a recent dramatic example. After its acquisition by Broadcom in 2023, VMware shifted its focus to the large enterprise sector, raising its prices and altering its support policies for smaller businesses, MSPs and VARs. These newly unfavorable terms encouraged many customers to seek a new hypervisor platform.

In any such migration effort, the alternatives are many, but getting there safely requires careful planning and the right tools. To properly protect itself, a business needs the ability to replicate and move its workloads freely — not just from one hypervisor to another, but from

Pricing increases and altered support policies have encouraged many VMware customers to seek a new hypervisor platform.

any physical server, hypervisor or cloud platform to another. This flexibility lets a business:

- Minimize its migration risk by enabling rollback from the new platform to the old one in the event of performance or reliability issues in the new environment.
- Improve its compliance posture with consistent backup, recovery and audit controls across physical servers, hypervisors and clouds.
- Improve its disaster recovery posture via replication of applications and data to the cloud.
- Scan backups in the cloud for malware and unpatched vulnerabilities, then mitigate those issues prior to recovery operations.
- Avoid vendor lock-in, moving workloads freely to new platforms as needed, e.g., when a hypervisor vendor raises its renewal and support prices.

The optimal solution provides these capabilities in one unified backup platform, thereby reducing IT licensing, training, integration and support costs.

Migration pitfalls on the road to a new platform

Consider the example of migrating from VMware to a new hypervisor. The steps are clear: Export the virtual machine (VM), convert it to the new hypervisor format and import it to the new platform. But each step in this transition adds potential challenges and cumulative risk, including differing virtual disk formats, chipset emulation models, virtual hardware versions, driver stacks and network virtualization layers. VM templates, snapshots and attached storage volumes behave differently. Compatibility issues may not arise until workloads are under production load.

Customers navigating the journey away from VMware routinely report serious issues from VM instability, network configuration problems, slow performance after conversion and the inability to fully revert if something goes wrong. The process of migrating from one hypervisor to another carries a real risk of turning into an expensive and protracted downtime incident. Other cross-platform moves, e.g., from one physical server to another or from a VM to the cloud, carry similar risks.

Hypervisor users have many attractive alternatives

To continue with the example of the unhappy VMware customer seeking an exit strategy, the market offers many worthy hypervisor alternatives, including:

Microsoft Hyper-V / Azure Stack HCI
a comfortable fit for companies already invested in the Windows and Azure ecosystem, offering tight integration with Active Directory, Azure security services and extant Microsoft licensing.

Proxmox VE
a popular open-source platform with transparent licensing, high availability features and an active user community.

Nutanix AHV
which offers simplified virtualization, storage and management under a unified platform with a predictable subscription model.

Scale Computing HC3
a hyperconverged platform optimized for edge environments like retail, manufacturing and distributed multisite environments with a focus on simplicity.

Other VM environments including Citrix XenSever, Red Hat Virtualization and Linux KVM.

But the process of migrating from VMware to any of these alternatives — and indeed of migrating any workload to a new physical, virtual or cloud platform — carries risks that businesses should anticipate and address before embarking on the journey.

Mitigating migration risk with the right data protection tools

Before embarking on a platform migration journey, businesses should consider investing in the right tools to help mitigate the potential risks. For example, a platform-agnostic backup solution can act as a safe conduit from VMware to Hyper-V, Proxmox, Nutanix or Scale Computing, or to non-hypervisor alternatives like physical servers and cloud platforms. A truly any-to-any backup solution, one that can ingest a workload from any source and restore it to any destination — from any physical, VM or cloud platform to any other physical, VM or cloud platform — can turn a treacherous offramp into a smooth glide path. Given the many potential hiccups cited in the VMware example above, it also must include the ability to quickly revert workloads to the original platform in the event of a performance, compatibility or operational problem.

In some cases, maintaining a hybrid old-and-new environment for a period of months can help hedge migration risk. This requires deployment of protection against data loss from a variety of possible causes (including ransomware, user errors and hardware failure) to ensure the business continues to honor its compliance and legal data retention obligations. An added benefit of these protections is freedom from vendor lock-in. If the new hypervisor solution doesn't work out in the long term, safe migration to another alternative is also possible in the future.

Acronis can make the off-ramp from old platforms smooth and risk free

For businesses ready to make such a transition, e.g., from VMware to an alternative hypervisor, Acronis has the tools to make the process simple, reliable, risk free and reversible. With the migration capabilities of the Acronis Cyber Protect platform and the optional help of Acronis Professional Services, businesses can enjoy:

- Migration options that can reduce transition time by as much as 60%, including direct agentless migration, mass migration with orchestrated execution and monitoring, and incremental migration via continuous synchronization to minimize business disruption.
- A zero-data-loss guarantee that ensures complete protection before, during and after migration.
- A unified platform for migration, backup and ongoing protection of the new environment.
- Cybersecurity validation to maintain security posture throughout the migration process.
- Quality assurance via post-migration validation of data integrity.
- A customized migration strategy designed by expert consultants for the business's unique environment.

Acronis Cyber Protect provides natively integrated cyber protection combining data protection, cybersecurity and endpoint management in a single platform. With a professional services team dedicated to VMware migration, Acronis offers 60% faster implementation, a data loss guarantee and a customized migration strategy.

To start the migration journey

1. Sign up for Acronis Cyber Protect to ensure complete protection.
2. Schedule a migration consultation with Acronis Professional Services experts.
3. Migrate with expert guidance, minimizing risks and disruption.

Protecting the new environment post migration

The same Acronis platform that enables safe migration from an old environment can also provide advanced backup and recovery capabilities for the new one, as highlighted in the table:

Secure, reliable backup for leading hypervisor alternatives to VMware

Hypervisor	Key Acronis backup features
Microsoft Hyper-V	Recovery of Hyper-V VMs to any system — including new, bare-metal or dissimilar hardware — with just a few clicks. Fast RTOs by running Hyper-V backups as VMs.
Nutanix	Efficient, low-impact, agentless protection for Windows and Linux VMs with full Prism integration, removing the need for guest agents and reducing overhead while ensuring consistent, reliable backups with Nutanix Ready Validation. Flexible storage options, including Acronis Cloud, Nutanix Objects / Files and third-party public clouds. Incremental backups and deduplication to cut storage costs. Backup scanning for malware that identifies harmful files to prevent reinfection during recovery. Scalability features to add or remove protected workloads as the business grows or reorganizes. Advanced encryption, role-based access control and immutability to support regulatory compliance and keep data safe from misuse. Full-image and file-level protection to capture entire Nutanix AHV virtual machines, optionally select certain files or folders for smaller, targeted backups, and ensure quick restores of full systems or individual items.
Proxmox	Efficient, low-impact, agentless backup for Proxmox VMs and LXC containers. File-level recovery and full system restores for fast, granular data protection. Flexible storage options including local disks, NAS devices, the Acronis Cloud and S3-compatible public clouds. Incremental backups and granular recovery to reduce backup windows and recovery times. Immutability, anti-malware scanning and FIPS 140-2 encryption to keep backup archives safe and compliant. Protection policies that can be auto-applied to new VMs and containers, eliminating gaps and ensuring every test or production environment is automatically backed up. Unified VM and container backup under one policy.
Citrix XenServer	Protection of XenServer workloads with complete disk-image backup. Elimination of operating system and application reinstallation in the event of a VM failure. Flexible storage options for XenServer VM backups in up to five locations, including local disks, NAS, SAN, tape and the Acronis Cloud.
Red Hat Virtualization (RHV)	Ability to restore RHV VMs in minutes to the same or another VM. Instant recovery of documents, files, folders or entire VMs directly from backup. Disk-image backup of RHV VMs that enables bare-metal restore to new hardware.
Linux KVM	Backup of Linux KVMs with disk-image backup of Linux hosts and agent-based backup of virtual machines. Protection management of all local and remote KVM hosts from one location with a single web-based management console.