DCIG

Data Mobility Imperative

Ensuring Agility, Resilience, and Recovery in Modern Hybrid Multi-cloud Environments

By DCIG Principal Analyst, Jerome Wendt

DCIG

TECHNOLOGY REPORT

Data Mobility Imperative

Ensuring Agility, Resilience, and Recovery in Modern Hybrid Multi-cloud Environments

Contents

Many underestimated the pain and costs that managing server virtualization, clouds, and hybrid multi-clouds and dealing with ransomware would incur.

A Shared Enterprise IT Vision

Many enterprises share a vision of what they want their modern IT infrastructure to look like. They want confidence and freedom:

- To deploy applications, data, and workloads anywhere in their hybrid multi-cloud environment: on-premises, in the cloud, or as-a-service.
- Their IT infrastructure will proactively identify issues and threats.
- They can dynamically keep applications, data, and workloads out of harm's way.
- They can optimize their available IT resources while lowering their costs.

While these objectives have universal appeal, they must simultaneously deal with the complexity of their current IT infrastructures. This creates at least four pain points that drive enterprises to seek data mobility. Further, and unfortunately, these pain points often impact enterprises in the worst possible way: their pocketbooks.

Today's Pain Points and Their Costs

Every enterprise knew that managing server virtualization, clouds, and hybrid multi-clouds and dealing with ransomware would create pain. However, many underestimated the amount of pain these four challenges would inflict and their associated costs. Consider:

Pain Point #1: Ransomware

Learning that a ransomware event has impacted their IT environment sends a chill through almost every enterprise. While enterprises have concerns about ransomware's impact on their IT environment and reputation, they often worry most about its cost.

Regardless of how ransomware attacks, the hackers behind it follow a familiar script. They inevitably demand a ransom from enterprises to decrypt their data, to suppress the release of exfiltrated data, or both.

While ransom amounts vary, the demand increasingly depends upon the business's annual revenue. Hackers often research companies before attacking and may seek a ransom of 1-5% of the company's annual revenue.[1] This has resulted in ransomware victims paying out $1 billion in 2023 with 2024 on pace to match it.[2]

Adding further insults to injury, enterprises receive no guarantees that after paying the ransom they will get their desired result(s). The provided decryption key may not work successfully, or the hacker may still release or sell the exfiltrated data. In either case, the ransomware event incurs substantial, unexpected out-of-pocket costs with no guarantee of successful resolution.

Further, paying a ransom does not account for the days, weeks, or months it often still takes enterprises to fully recover. The costly and unpredictable nature of ransomware events has prompted most enterprises to deploy even more robust cybersecurity defenses. However, if compromised, most prefer better, more cost-effective and reliable recovery options than negotiating with hackers.

Many enterprises have neither explored nor identified viable VMware alternatives. This has forced many to remain with VMware, at least for now.

Pain Point #2: Server Virtualization Dependency

Selecting VMware as their server virtualization platform once represented an almost de facto choice for enterprises. No more. Skyrocketing VMware server virtualization costs now appear on many enterprise radar screens.

Broadcom's VMware software licensing changes highlighted how much enterprises took VMWare's prior software licensing model for granted. VMware's predictable percentage year-over-year (YoY) increase has now doubled, tripled, or jumped by 10x from some.[3]

Aggravating the situation, many enterprises have neither explored nor identified viable VMware alternatives. This has forced many to remain with VMware, at least for now.

Yet even as enterprises begin to identify alternatives, they possess limited or no means to switch to another server virtualization platform. Even assuming a change from VMware to another platform, will a similar situation again arise, that requires yet again another switch?

Pain Point #3: Cloud

Many enterprises initially embraced the cloud anticipating benefits such as increased agility, availability, performance, security, and resilience. While many organizations experienced these cloud benefits, they also encountered some of the cloud's downsides.

The amount of cloud resources utilized coupled with the types of applications deployed contribute to enterprises struggling with cloud costs. The complexity associated with managing applications in the cloud and cloud resources contributes to escalating cloud costs. 60 percent of organizations saw their cloud costs rise with 40 percent experiencing increases of more that 25 percent.[4]

This has prompted many enterprises to examine ways to mitigate or even eliminate their cloud costs. To reduce their reliance on a specific cloud provider, they may take one or more of the following actions:

- Repatriate some or all applications and data on premises.
- Repatriate some or all applications and data with one or more cloud providers.
- Modernize some or all existing applications by re-deploying them on containers and then hosting them in Kubernetes environments.
- Building applications in platform as-a-service (PaaS) environments to obtain the key cloud benefits they need without needing to manage an entire cloud environment.

Enterprises may find that taking one or more of these steps only serves as a bandage. It may temporarily reduce their overall cloud costs though even that is not guaranteed.

If anything, they often find that spreading their applications and data across all these environments only increases their management complexity. This results in cloud costs resurfacing, backups and recoveries becoming more difficult to complete, or compromises in their IT cybersecurity perimeter occurring.

Absent a defined plan to address these follow-on challenges, they only complicate and perhaps worsen their cloud management.

Modern data mobility represents a viable path forward to addressing today's modern enterprise pain points.

Pain Point #4: Hybrid Multi-cloud Environments

As enterprises look to control and manage costs, almost 90 percent already adopt hybrid multi-cloud IT environments.[5] In these environments, enterprises host applications and data on premises plus across two, three, or more public clouds. These clouds may encompass both general-purpose public clouds that offer multiple cloud services and purpose-built clouds with only one cloud service.

Using multiple clouds gives enterprises access to the benefits that each cloud provider offers. Price, performance, or specific cloud features can each contribute to enterprises opting to adopt different clouds to address specific needs.

Unfortunately, hybrid multi-cloud configurations can lead to enterprises re-introducing management complexity into their IT environments. This puts them in a quandary. They need the features that hybrid multi-cloud environments offer. However, they must now mitigate re-introducing management complexity into them.

Modern Data Mobility: A Viable Path Forward

Modern data mobility represents a viable path forward to addressing these four enterprise pain points. While it continues to facilitate migrating or moving applications and data from one physical platform to another, it now does much more

All four modern pain points listed above stem from, in part, the inability of enterprises to either act or respond effectively. Enterprises:

- Must pay ransoms because they have limited or no options to quickly recover compromised production data.
- Must pay higher cloud and server virtualization costs since they can neither easily nor effectively transition to other platforms.
- Encounter increased management complexity and costs in hybrid multi-cloud environments due to lack of a single solution that can identify, orchestrate and then move and migrate applications and data across this environment.

These issues highlight how data mobility as a technology must modernize to meet the IT needs of today's enterprises. Few if any enterprises only use one hypervisor or one cloud anymore. Rather, they find themselves enmeshed in hybrid multi-cloud environments. As such, they need a data mobility solution optimized for these environments.

To do so, modern data mobility must facilitate and enable cloud and hypervisor platform independence. This approach equips enterprises to freely migrate and move their applications and data between different hypervisors and clouds.

It also permits business requirements to drive technological decisions, not technical specifications to drive business decisions as may occur now. This gives enterprises freedom to migrate and move applications, files, objects, and virtual machines (VMs) to wherever they need them.

Hybrid multi-cloud data mobility begins with the premise that enterprises can theoretically move their data between any platform, wherever and whenever.

Data Mobility Defined for Hybrid Multi-cloud Environments

Data mobility has always had a certain appeal to it. It may begin with the premise that enterprises can theoretically move their data between any platform, wherever and whenever. Unfortunately, achieving this data mobility ideal has proven elusive as, to date, data mobility has its limits.

Its current limitations demand that one first define data mobility in the context of how one plans to use it. As almost all enterprises now possess hybrid multi-cloud environments, they need a data mobility solution appropriate for them. This requires a data mobility solution that ideally supports and delivers on the following three capabilities:

- ***Capability #1: Can move files and/or objects between different hypervisors and cloud platforms.*** This may represent the simplest objective to achieve. Many existing software offerings that position themselves as data mobility solutions exemplify this. They already support file and object movement between different hypervisors and cloud platforms. They can often move files or objects anywhere at any time either on premises, offsite, or to any number of clouds. In this case, support of specific hypervisors or clouds has little bearing on its ability to deliver this functionality.
- ***Capability #2: Can move virtual machines between different hypervisors or cloud platforms.*** Moving a VM from one hypervisor to a different hypervisor or cloud platform represents yet another form of data mobility. This represents a more complex form of data mobility as it includes elements of both data movement and data migration.

  One must first quantify both the environment in which the VM currently resides and the new environment. The migration will then move the VM in such a way that it successfully operates on the new platform. This migration often must convert the VM's configuration, identity, networking, security, and storage to operate on the new platform.

  Due to these additional requirements, the data mobility solution should ideally assess the likelihood of success in making such a move. It should also offer options to fail back should the VM migration fail or the VM does not operate as expected.
- ***Capability #3: Can move virtual machines to PaaS or serverless environments.*** More enterprises have started to modernize their IT environments. Taking this route, they may move existing virtual machines to a PaaS, to containers in a serverless environment, or both.

  Moving to PaaS does not allow for a direct migration of VMs. Enterprises will first need to understand all the VM's application dependences, configurations, and resource usage. Migrating VMs with databases to PaaS will often require moving to a managed database service offered by PaaS. Alternatively, enterprises will need to move to a separate database platform.

  Migrating VMs to a serverless environment requires an even higher degree of sophistication to successfully execute. Enterprises must still document and understand each VM's application dependences, configurations, and resource usage. However, they must also assess, understand, and determine if they can move the VM from a state***ful*** to a state***less*** environment.

A data mobility solution that offers all three of these capabilities becomes almost imperative in hybrid multi-cloud environments. However, enterprises should also set realistic expectations.

For instance, they should not expect the solution to include options to move data between application platforms. For instance, they should not expect it to move data from a SaaS application such as M365 to Google Workspace. They also should not expect it to handle database migrations such as from Oracle Database to Amazon RDS.

Seven Requirements of a Hybrid Multi-cloud Data Mobility Solution

The freedom to move and migrate applications and data in hybrid multi-cloud environments makes data mobility imperative. Without it, enterprises will always struggle in responding to ransomware, avoiding cloud and server virtualization platform dependencies, or unlocking the benefits of hybrid multi-cloud environments. Therefore, choosing a data mobility solution that can deliver on these imperatives requires it minimally possess the following seven attributes.

Enterprises should begin to view and manage data mobility software in the same context as data protection software.

Attribute #1: Data Mobility and Data Protection Software Become One

Backup and recovery no longer represent one-off processes that enterprises manage. Driven by ransomware events and heightened user expectations, enterprises now centrally manage and treat data protection as a core IT process.

However, enterprises should begin to view and manage data mobility software in the same context as data protection software. Too often they implement and manage data mobility and data protection software separately despite these two solutions sharing some traits. For instance, data protection software itself can often protect:

- Data and objects on one file system or object store and then restore or ***migrate them*** to another.
- VMs on one hypervisor or cloud platform and then restore ***or migrat***e them to another.
- Containers that reside on one Kubernetes platform and then restore ***or migrate*** them to another.

Further, enterprises already routinely deploy and use data protection software. Identifying data protection software that includes robust data mobility capabilities positions them consolidate data protection and data mobility into one solution.

Attribute #2: Supports Primary Hybrid Multi-cloud Platforms

A data mobility solution for a hybrid multi-cloud environment must minimally support the primary platforms found in such an environment.

On the cloud side, enterprises should expect a solution to support Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. On the hypervisor side, enterprises should similarly expect support for Azure Stack, Microsoft Hyper-V, Nutanix AHV, and VMware vSphere.

Beyond cloud and hypervisors, the solution should provide a viable roadmap for supporting other platforms. While that roadmap should include supporting other clouds and hypervisors, it may include a roadmap for migrating to PaaS, SaaS, and serverless environments.

To support PaaS and serverless environments, a data mobility solution must do more than simply lift-and-shift virtual machines. It will ideally provide options to refactor VMs that enterprises may then deploy and host on either PaaS or serverless platforms. If available, a data mobility solution offering this functionality may only support a few PaaS or serverless platforms.

The same condition applies if looking to migrate SaaS applications to other platforms. Enterprises should currently only expect to find data mobility for SaaS applications as a

roadmap feature. If available now, it will again only support a few SaaS applications, such as migrating from Microsoft 365 to Google Workspace.

However, the number of enterprises adopting SaaS may lead to data mobility solutions supporting SaaS apps other than collaboration solutions. It may support data mobility for DevOps SaaS applications such at GitHub or Atlassian Cloud or IAM SaaS applications such as Entra ID.

Enterprises need flexibility in how they deploy their software which stems from how quickly their IT infrastructure can change.

Attribute #3: Multiple, Flexible Deployment Options

In today's modern IT environments, enterprises need flexibility in how they deploy their software. This need stems from how quickly enterprise IT infrastructures can change.

Enterprises can rarely accurately predict exactly which deployment option they may need over time. Further, enterprises may utilize many or all deployment options available in a software solution.

These dynamics often dictate that a data mobility solution supports multiple deployment options. These options may include deploying the data mobility solution as:

- A physical or virtual appliance.
- A SaaS offering.
- Managed service.
- Software for deployment in the cloud, on-premises, or both.

Attribute #4: Cohesive Management

A data mobility solution that offers multiple deployment options may give enterprises the flexibility they may need. However, deploying the solution in multiple ways can also result in it becoming complex to manage and improperly secure. This may occur if an enterprise must log into each deployment of the solution to manage, maintain, and secure it.

A data mobility solution that offers a central, cloud-based management console hosted by the provider can overcome this potential drawback. This central console should cohesively manage the data and security functions that the data mobility solution offers.

To do so, the console must access and manage all the deployments of the data mobility solution. In this role, the central console manages data placement but more importantly handles security at multiple levels across the various deployment types.

For instance, it can centrally schedule anomaly scanning and detection and manage alerting for ransomware detection. It can also manage intrusion detection by handling identity and access management (IAM) across all the deployments. These functions can include managing user roles at specific locations, supporting multi-factor authentication (MFA), or delivering multi-tenancy.

Attribute #5: Flexible, Resilient, Scalable Architecture

A data mobility solution that offers multiple deployment options represents only one type of flexibility. The IT infrastructure of enterprises with hybrid multi-cloud environments changes constantly. Enterprises may experience organic growth in one location or expand into new locations. They may contract or close other locations. They may only need some locations temporarily.

In order for data mobility to assume an expanded role in enterprises they must find it affordable.

To accommodate these different requirements, the data mobility solution must inherently provide a flexible, resilient, scalable underlying architecture. In addition to supporting multiple deployment options, this architecture should enable the solution to scale up or down as needed.

In this way, should enterprises encounter performance spikes, unexpected growth, or unforeseen contraction, the solution can handle these events.

The data mobility solution should also include features that permit it to move or migrate different data types. While it must handle virtual machine moves, migrations, and restorations, enterprises can also move, migrate, and restore other data types.

These include block, file, and object data that they could move or migrate at any time. As such, the solution must also offer deployment options while remaining available 24x365x7.

Attribute #6: Cost-effective

Enterprises typically only acquire a specific data mobility solution when they have a specified, quantifiable need for it. Even then, they typically first check the capabilities of other in-house software they own before they buy it. It simply does not represent software that enterprises buy and keep around *"just in case"* they need it.

However, recent events such as Broadcom's VMware software licensing changes have prompted enterprises to re-examine this mindset. Further, as more enterprises implement hybrid multi-cloud environments, the need for data mobility software may switch from *"nice-to-have"* to *"must-have."*

Capitalizing on the benefits that a hybrid multi-cloud environment offers requires a solution that can move data around within it. However, for a data mobility solution to assume this expanded role, enterprises must find it affordable.

Attribute #7: Accounts for Unaccounted Pockets of IT

Demanding a product includes a feature that accounts for the unaccountable sounds like an oxymoron. After all, how can data mobility software account for a component of enterprises that they themselves struggle to account for?

Normally, meeting this request would be impossible. However, in this case, data mobility software can make provisions to account for the divisions that exist within enterprises. These include DevOps, edge IT, and shadow IT that do often exist in many enterprises.

These divisions or aspects of enterprises sometimes represent the Wild West of IT. Granted, innovation tends to occur rapidly here. At the same time, these parts of an enterprises introduce security risks.

They likely do not have good processes in place to backup and restore their data. They may use SaaS applications that have corporate data hosted in other providers' clouds. However, enterprises sometime need to bring these *"rogue"* IT environments under centralized control.

The challenge then becomes two-fold. First, enterprises must identify and quantify the applications and data that exist on the outskirts of their IT infrastructure. Once quantified, they need a means to move or bring these applications and data under central IT management.

Using the same R-Cloud solution that protects applications, data, and VMs, enterprises also obtain the modern data mobility capabilities they now need.

HYCU R-Cloud: Delivering on the Data Mobility Imperative

HYCU represents one of the first technology providers to recognize the growing role that data mobility plays in data protection. By offering data mobility as a core feature in R-Cloud, enterprises can look to utilize HYCU R-Cloud™ more extensively.

R-Cloud already provides the core features that enterprises expect and demand of enterprise software. As a data protection solution, R-Cloud:

- Protects and restores applications, data, and VMs across all primary cloud and hypervisor platforms.
- Protects and restores applications, data, and operating systems hosted on physical servers.
- Offers multiple deployment options that include SaaS, software, virtual appliances, and more to meet various enterprise requirements.
- Through these multiple deployment options, it gives enterprises different levels of flexibility, resilience, and recovery options they need.
- Provides a centralized, cost-effective cloud console that can discover and manage existing IT environments.
- Equips organizations to bring rogue IT operations under centralized management at the right time.

Using HYCU R-Cloud, enterprises could already protect applications, data, and VMs regardless of where they resided in their IT infrastructure.

Now using the same R-Cloud solution, enterprises obtain the modern data mobility capabilities they now need. This approach mitigates or even eliminates the need to acquire either new backup or data mobility software.

Using R-Cloud enterprises may move data *(files, objects, and VMs)* almost anywhere they need across much of their hybrid multi-cloud environment. Further, it gives them new freedom to migrate data, to include VMs, across multiple hypervisors and clouds.

Data Mobility Imperative: Ensuring Agility, Resilience, and Recovery in Modern Hybrid Multi-cloud Environments

Enterprises today find themselves dealing with four major pain points—often simultaneously. Be it ransomware, server virtualization lock-in, cloud lock-in, or hybrid multi-cloud environments, responding to any one of these can feel overwhelming. Then when asked to provide additional benefits from their hybrid multi-cloud environment, they may find that request challenging, at best, to meet.

An effective, holistic data protection and mobility solution changes these dynamics. At a minimum, data mobility addresses these four pain points that almost every enterprise now faces. Equally important, it helps unlock the latent value that hybrid multi-cloud environments offer. By obtaining a combined robust data protection and mobility solution, enterprises now get the best of both worlds.

Data protection software already possesses the core functionality that enterprises expect and need enterprise software to deliver. Whether these requirements entail high availability, multiple deployment options, support for multiple cloud and hypervisor platforms, centralized cloud console, or other features, enterprise data protection software delivers on them.

By introducing data mobility into enterprise data protection software as another option, enterprises can now meet their data mobility imperative.

HYCU bringing data protection and data mobility together in R-Cloud illustrates the impact of this combination of technologies.

HYCU bringing data protection and data mobility together in R-Cloud illustrates the impact of this combination of technologies. R-Cloud puts enterprises in control of more than just the protection of their data and VMs across their environment. It also puts them in control of the movement of these items across their hybrid, multi-cloud environment.

HYCU R-Cloud effectively positions enterprises to meet today's data mobility imperative. Using R-Cloud's existing, proven architecture, enterprises may immediately deploy and start using it.

In so doing, they begin to achieve the levels of agility, resilience, and recoverability they expect from their hybrid, multi-cloud environment. Just as important, they can do so cost-effectively while mitigating the introduction of new complexities into their IT environment. ■

Sources

1. https://www.mindpointgroup.com/blog/the-costs-of-a-data-breach. Referenced 1/14/2025.
2. https://therecord.media/ransomware-payments-doubled-to-more-than-1-billion-2023. https://therecord.media/ransomware-gangs-set-record-for-money-extorted. Referenced 1/18/2024.
3. https://arstechnica.com/information-technology/2024/12/company-claims-1000-percent-price-hike-drove-it-from-vmware-to-open-source-rival/. Referenced 1/14/2025.
4. https://www.cio.com/article/3496509/rising-cloud-costs-leave-cios-seeking-ways-to-cope.html. Referenced 1/15/2025.
5. https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-2024-state-of-the-cloud-report/. Referenced 1/18/2025.