Technology Report

DCIG

Getting Data Protection Right in a Hybrid Data Center

By DCIG President & Founder, Jerome Wendt

DCIG

TECHNOLOGY REPORT

Getting Data Protection Right in a Hybrid Data Center

Contents

The Emergence of the Hybrid Data Center

The emergence of the hybrid data center should come as no surprise. A hybrid data center utilizes virtualization, cloud, and software-defined offerings spread across both cloud and on-premises data centers. This comprehensive approach provides the benefits of each deployment type while addressing their specific drawbacks.

Yet perhaps more importantly, a hybrid data center provides organizations increased flexibility to meet changing and emerging trends and requirements. Many of them directly impact how they host and manage their IT operations. These include technology innovations, cultural shifts in employee behavior, emission reductions, and ransomware threats, among others.

> ***"A hybrid data center provides organizations increased flexibility to meet changing and emerging trends and requirements."***

Adapting to these forces on the fly dictates organizations create an adaptable, flexible IT environment. A hybrid data center provides a viable and practical way for organizations to respond. However, implementing and supporting a hybrid data center creates specific management challenges.

For instance, organizations must:

- Protect and secure applications and data both in the cloud and on-premises
- Recover applications and data in either the cloud or on-premises regardless of where they were originally hosted
- Manage backup and recovery functions across this environment

Successfully meeting the specific demands of a hybrid data center requires deploying a data protection solution tuned to meet them.

Events and Trends Driving Hybrid Data Center Adoption

Many of the events and trends from the years 2000 through 2020 reshaped the workplace going forward. While not a comprehensive list, some have specifically contributed to the need for organizations to adopt a hybrid data center model. These include:

- ***Hosting workloads in public clouds.*** Organizations rapidly adopted public clouds from 2010 to 2020 moving many of their applications and data into them. Public clouds provided them with secure, stable, highly available IT environments. They also facilitated fast application deployments and easy scaling of compute and storage resources.
- ***Continuing to host workloads on-premises.*** Despite the public clouds' many benefits, organizations often remain ill-equipped to effectively manage public cloud environments and control costs. Keeping workloads on-premises help address these concerns. Further, new cloud technology offerings exist that can host workloads on-premises. These offer key public cloud benefits such as high availability, ease of scaling, and dynamic resource allocation and reclamation.
- ***Climate change and emissions control initiatives.*** The Glasgow Climate Pact agreed at the 2021 COP26 UN Climate Change Conference to begin addressing concerns about emissions and their environmental impact. For instance, it laid out steps to reduce the cooling industry's climate impact and drive action on reducing methane emissions.[1] As these initiatives become regulations, organizations must prepare to respond.
- ***New employee workplace expectations.*** The COVID-19 pandemic of 2020-21 turned the conventional workplace upside down. Many organizations adapted their work environment to support their employees working remotely. As a result, many employees expect to work remotely in some capacity indefinitely.

- ***Supply chain issues.*** The pandemic exposed the many dependencies that exist in the worldwide supply chain. These issues negatively impacted the availability of core technologies upon which organizations rely to maintain a reliable IT infrastructure.
- ***Employee availability.*** Both worker shortages and COVID-19 resurgences impact employee availability. Worker shortages make finding and retaining employees difficult. Once employed, COVID-19 resurgences may prevent employees from working for extended periods.
- ***Ransomware's threat.*** Every organization recognizes the threat ransomware presents to its business and IT operations. Further, cybersecurity experts agree ransomware will continue to become more pervasive. To guard against it, organizations must protect and secure workloads wherever they reside, in the cloud or on-premises.

These events and trends, among others, contribute to organizations embracing a hybrid data center. A hybrid data center gives them more options to meet unexpected demands in a rapidly changing world.

Getting Data Protection Right in a Hybrid Data Center

Getting data protection right in a hybrid data center puts a spotlight on specific data protection attributes. The task of protecting applications, data, and workloads hosted in a hybrid data center itself presents specific challenges. The solution must also equip organizations to perform multiple other tasks associated with data protection. Adding to the dilemma, the need for some of these features only surfaces in a hybrid data center environment.

Any data protection solution being considered for protecting a hybrid data center should therefore ideally deliver on the following five attributes.

> ***"The use of backups to successfully recover from ransomware attacks has put backup software in hacker's sights."***

#1: Secures Backups from Ransomware

The use of backups to successfully recover from ransomware attacks has put backup software in hacker's sights. If hackers can compromise backups or the backup software, they increase their odds of obtaining a ransom. In response, backup software used in a hybrid data center should offer features that mitigate and repel these attacks. These include:

- ***Securing access to backup software.*** The backup software should authorize and authenticate any individuals that access the backup software. Using available multifactor authentication (MFA) technologies, the backup software first verifies the user's identity. It should then utilize identity and access management (IAM) to control and monitor user actions. It may even require approvals of multiple individuals to perform certain tasks, such as changing backup schedules or deleting backups.
- ***Managing immutable storage***. The backup software should possess the ability to manage available immutable storage technologies. These offerings store backups in a readable, but unchangeable, format to prevent ransomware from encrypting it. Organizations may obtain immutable storage offerings that operate either in the cloud or on-premises. Immutable cloud storage utilizes the object lock feature already found on many cloud object storage offerings. On-premises offerings operate in a similar manner. They deliver object storage on-premises with object lock functionality.
- ***Scanning backups for ransomware***. The backup software ideally offers the option to scan backup data for ransomware. Ransomware can and does slip past production cybersecurity software, such as antivirus software and firewalls. Scanning data for ransomware during backups and recoveries and minimally alerting to its presence provides additional protection against ransomware.

#2: Multiple Deployment Options

Organizations will likely need multiple options to deploy backup software in a hybrid data center. Whether they perform backups in the cloud, on-premises, or both may influence how they deploy the backup software. However, even when deploying in just one of these environments, they may want a choice of deployment options. Organizations have different sizes and types of on-premises environments they need to protect for which they will need different implementation options.

To meet these different needs, organizations should establish which deployment options the backup software offers. Ideally, it will offer as many of the following as possible to give them the most flexibility.

- Backup appliance (physical, virtual, or both)
- Backup-as-a-service (BaaS)
- Software license

#3: Workload Mobility

In a hybrid data center, workloads may reside in the cloud, on-premises, or both. This requires a data protection solution to do more than simply identify where the workload gets backed up. It must also recognize the environment into which it gets recovered. This recognition becomes essential for it to take the prerequisite steps to appropriately recover a workload in the cloud or on-premises.

#4: Leverages Available APIs

The underlying cloud and on-premises environments in which workloads reside each offer multiple application programming interfaces (APIs) for management. Backup software may use some of these APIs to more effectively, and efficiently, back up and recover VMs.

"Successfully implementing data protection in a hybrid data center makes centralizing backup management a prerequisite."

#5: Centralized Backup Management Console

Successfully implementing data protection in a hybrid data center makes centralizing backup management a prerequisite. To meet this demand, the backup offering must offer its own centralized backup management console.

Backup software providers often integrate their backup software with the management consoles that cloud, hypervisor, and operating system providers offer. These integrations make it easier to manage backups as part of managing operations in a specific environment. However, a cloud-, hypervisor- or operating system-centric approach for management becomes impractical in a hybrid data center.

In a hybrid data center, a centralized backup software console manages backup and recovery across both the cloud and on-premises. Implemented this way, organizations only need a single console to monitor and manage backups and recoveries across a hybrid data center.

This single management console facilitates administering backup and recovery tasks such as:

- Identifying the workloads that run in each environment
- Recognizing the service level agreements (SLAs) that may exist in each environment
- Setting policies specific to each environment as well as one that works across the entire environment

> *"A proven enterprise backup software, Arcserve Unified Data Protection (UDP) comes equipped to protect a hybrid data center."*

Arcserve UDP: Tuned for Hybrid Data Center Protection

A proven enterprise backup software, Arcserve Unified Data Protection (UDP) comes equipped to protect a hybrid data center. UDP has continued to add features to better position it to protect a hybrid data center. Its enhancements manifest themselves in the following ways.

Secured by Sophos

Through a strategic alliance with Sophos, multiple Arcserve offerings include the Secured by Sophos moniker. This integration offers additional cybersecurity functionality to help organizations defend against ransomware.

Arcserve offerings covered include its UDP Software, Appliances, UDP Cloud Hybrid, and Cloud Backup for Office 365. Using this Secured by Sophos integration, all Arcserve offerings proactively monitor for ransomware and respond to attacks.

Air-gapped Technology Management

Arcserve's offerings manage the various, available air-gapped technologies. These technologies offer a proven method to protect backups from ransomware. They logically or physically segment backups from the production environment. Logical air gaps use immutable storage offerings that may reside in the cloud or on-premises. Physical air gaps place data on disk or tape media that organizations may physically disconnect from the production environment.

Encrypts Backups At-rest and In-flight

Hackers have added a new twist to their ransomware attacks. Some ransomware strains exfiltrate data and send it to the hacker before encrypting it. Hackers then threaten to publicly release this exfiltrated data unless organizations pay a ransom. To make backups unreadable and unusable for a public data release, organizations may use any Arcserve offering to encrypt backups whether at-rest or in-flight.

Authenticated User Access and Changes

Ransomware may also compromise backup processes by logging into the backup software to turn off backup jobs or delete backups. To deter these attempts, Arcserve provides multiple options to secure access to its backup offerings. It supports the creation of complex administrative and user passwords as well as multi-factor authentication (MFA). Once admins and users log into Arcserve, it continues to monitor and control their activities through role-based access controls (RBAC).

Multiple Deployment Options

The needs of enterprise organizations constantly change in terms of the types of environments they need to protect. These evolving requirements dictate they select a data protection solution that gives them multiple options to deploy it. Arcserve meets this need. Organizations may acquire and deploy Arcserve offerings as either a licensed software offering or as a backup appliance.

Workload Mobility Using Available APIs

The flexibility to back up and recover workloads in either a cloud or on-premises environment is not a nice-to-have. It is a must-have. Arcserve delivers on this hybrid data center requirement.

Arcserve backs up physical machines and then restores them to virtual machines (VMs) hosted either on-premises or in the cloud. Arcserve also protects and recovers virtualized application workloads whether organizations host them on-premises or in the cloud. Arcserve integrates with available cloud, hypervisor, and operating system APIs to perform these backups and recoveries.

Single Management Interface

Arcserve offers a single console to manage data protection across the entirety of a hybrid data center. Once logged in, administrators and users may monitor and manage backups and recoveries for workloads running both on-premises and in the cloud. Equally important, they may centrally create policies and then apply them as appropriate in each type of environment.

Company	**Arcserve**
Location	8855 Columbine Road Suite 150 Eden Prairie, MN 55347
Phone	(844) 765-7043
Website	https://www.arcserve.com/

Arcserve UDP Meets the New Dynamics of Hybrid Data Center Data Protection

Organizations that adopt and implement a hybrid data center join many others in this trend. Only a hybrid data center gives organizations the option to experience the benefits of both on-premises and cloud data centers. Further, they gain the flexibility to move workloads from the cloud to on-premises or vice versa.

However, this flexibility to host workloads in the cloud and on-premises changes the dynamics of data protection. Data protection solutions that work well in the cloud or on-premises may display gaps when protecting a hybrid data center. These gaps may specifically show up in ransomware protection, deployment options, workload management, and centralized management.

Arcserve recognized this enterprise trend toward hybrid data center adoption and enhanced its offerings accordingly. It struck an alliance with Sophos to deliver many of its offerings Secured by Sophos. This ensures organizations secure their backup data from ransomware when they use an Arcserve Secured by Sophos offerings.

Arcserve further enhances its Sophos alliance with its own set of security measures. It authorizes and authenticates user access and actions. It facilitates centrally protecting and recovering data across both cloud and on-premises environments, using available APIs. It encrypts backup data both at rest and in-flight and gives organizations the option to store this data on air-gapped technologies.

Arcserve's management and security features collectively position organizations to meet the dynamic data protection requirements of a hybrid data center. ■

> ***"Arcserve's management and security features collectively position organizations to meet the dynamic data protection requirements of a hybrid data center."***

Sources

[1] https://www.unep.org/news-and-stories/story/cop26-ends-agreement-falls-short-climate-action. Referenced 3/28/2022.

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. Please visit **www.dcig.com.**