

DCIG TOP 5

Azure Cloud Backup Solutions

by DCIG President and Founder, Jerome M Wendt



TOP 5 Azure Cloud Backup Solutions*

Zerto IT Resilience Platform

Cobalt Iron Compass

Commvault Backup and Recovery

HYCU for Azure

Unitrends Backup

* Licensing provider listed first.
Others listed in alphabetical order.

SOLUTIONS EVALUATED:

- Arcserve Unified Data Protection (UDP)
- Cobalt Iron Compass
- Cohesity DataProtect
- Commvault Backup and Recovery
- HYCU
- Microsoft Azure Backup
- Novastor NovaBackup
- Quest NetVault Plus
- Rubrik Cloud Data Management
- Unitrends Backup
- Vembu
- Zerto IT Resilience Platform

SOLUTION FEATURES EVALUATED:

- Backup administration
- Backup capabilities
- Configuration, licensing, and pricing
- Recovery and restores
- Snapshot administration
- Support

Microsoft Azure Going Neck and Neck with AWS

For years Amazon Web Services (AWS) seemed to possess an almost insurmountable lead in the public cloud infrastructure-as-a-service (IaaS) provider market. Then, Microsoft Azure made some changes to its public cloud offerings. Led by its SaaS-based Office 365 and IaaS-based Azure offerings, Microsoft closed the gap to now go neck and neck with AWS. Consider:

- Microsoft Office 365 is the cloud software-as-a-service (SaaS) most used by enterprises¹
- 69 percent of enterprises currently use Azure compared to 76 percent of them using AWS²
- 63 percent of all size organizations use Azure compared to 76 percent of them using AWS³
- Microsoft Azure generated about \$8 billion in revenue in 2019, second only to AWS⁴

Since 93 percent of enterprises already have a multi-cloud strategy, this bodes well for Microsoft Azure's continued adoption and growth.⁵ Microsoft Azure offers all size organizations a viable public cloud choice with some of the best options available to host Microsoft applications.

Microsoft Azure provides the core IaaS services that many enterprises initially seek to create a viable multi-cloud strategy. These core services include analytics, compute, database, identity management, networking, storage, virtual desktops, and web. Azure also offers advanced services such as artificial intelligence, containers, DevOps, Kubernetes, machine learning, and serverless, among others.

As of September 2020, Microsoft Azure has nearly 50 regions throughout the world with seven more in development. 10 of these regions include availability zones. Taken together, these benefits make a compelling argument for enterprises to adopt, embrace, and expand their use of Azure.

Backup Still a Requirement in the Azure Cloud

Microsoft Azure offers many features organizations want from a public cloud platform to include high availability, redundancy, security, and many more. Despite the benefits Azure offers, organizations must keep one principle in mind: they retain responsibility for their data.

This puts the onus on organizations to back up and recover their data. Should their data get corrupted, deleted, lost, or compromised, they need a solution in place to protect it.

Microsoft does offer its own Azure backup service. However, it is a separate offering designed to back up virtual machines in the Azure cloud to which organizations must subscribe. Many organizations will have application and data requiring specific backup and recovery features beyond what the Azure backup service offers. This will necessitate they acquire a third-party solution that meets their Azure backup and recovery needs.

The State of Azure Cloud Backup Solutions

Despite Microsoft Azure's prominence as an IaaS provider, organizations have small number of backup solutions from which to choose. Ten of these solutions got their start doing physical or virtual machine backup. This start gave them the core functionality that organizations still need as they move existing applications to the cloud.

Organizations deploy these backup solutions in the Azure cloud the same way they do on-premises, with minor differences. They obtain an appropriately sized Virtual Machine instance from Azure to host the backup software. They license, install, and maintain the backup solution themselves. They configure it to back up their applications hosted in the Azure cloud. In many respects, they manage this backup software in the cloud the same way they do now.

1. <http://technalysisresearch.com/downloads/TECHnalysis%20Research%20Hybrid%20and%20Multi-Cloud%20Study%20Highlights.pdf>. Pg 6. Referenced 9/6/2020. Hybrid and Multi-cloud Study: The New Enterprise Computing Reality. Technalysis Research.
2. <https://resources.flexera.com/web/pdf/report-state-of-the-cloud-2020.pdf>. Pg. 52. Flexera 2020 State of the Cloud Report.
3. Ibid. pg. 51.
4. <https://www.gartner.com/en/newsroom/press-releases/2020-08-10-gartner-says-worldwide-iaas-public-cloud-services-market-grew-37-point-3-percent-in-2019>. Referenced 9/6/2020.
5. Ibid. pg. 10.

Azure cloud backup solutions delivered this way do, however, face a challenge going forward. Fewer organizations want to manage backup software the same way they did in the past. Instead, they want to subscribe and pay for backup software like they do other services in the Azure cloud.

They also want backup software architected and available as a cloud-native service. Delivered this way, the backup software automatically scales up or down based on demand. The provider also handles all the backup software's ongoing maintenance, such as fixes, patches, and upgrades. This frees organizations to focus on using the backup software while removing the task of maintaining it.

Of the twelve Azure cloud solutions DCIG evaluated, two got started in Microsoft Azure as a cloud-native Azure software-as-a-service (SaaS). They deliver this cloud-native backup SaaS offering that organizations seek. The main challenge cloud-native offerings often face is they lack robust backup features for applications that organizations lift-and-shift to Azure.

As these cloud-native SaaS offerings deliver on this requirement, they will become more attractive to organizations. Conversely, expect more current providers to make their software available as SaaS-based, cloud offerings in the coming years. Already five cloud backup offerings make their software available as a SaaS-based offering that runs outside of the Azure cloud.

Common Features Across All Azure Cloud Backup Solutions

DCIG identified twelve solutions in the marketplace that offer backup capabilities for the Microsoft Azure cloud. These solutions target organizations of various sizes based on the capabilities described in their User Guides or published data sheets. Due to the recent introduction of many Azure cloud backup offerings, features they all share remain negligible. Attributes that all these solutions had in common include support for the following:

1. **Back up all Windows Server versions from 2008 forward.**

Organizations may choose from multiple Microsoft Windows operating systems (OSes) to host their VMs in the Azure cloud. Any of these backup solutions will protect applications hosted on any Microsoft Windows OS released since 2008.

2. **Back up Red Hat Enterprise and SUSE Linux.** Organizations may also select from among seven Linux releases available in the Azure cloud. These twelve backup solutions only universally support Red Hat Enterprise and SUSE Linux releases.

3. **Perform incremental and full backups.** Every backup solution gives organizations the option to perform full and incremental backups. They create a first full backup and then do incremental backups thereafter.

4. **Protect Windows file servers.** Many organizations continue to use the Windows file sharing feature to share files between users. All twelve solutions equip organizations to back up and recover files stored on Windows file servers.

Similarities between the TOP 5 Azure Cloud Backup Solutions

In addition to the features listed above, all TOP 5 Azure cloud backup solutions have the following traits in common. They include:

- **Back up and recover non-Azure databases such as MySQL, Oracle Database, and SAP HANA hosted in Azure.** Organizations

Next Gen Azure Cloud Backup Solution Features

Providers remain in the early stages of optimizing their software to back up and recover applications and data hosted in Azure. As a result, the breadth and type of features they offer that leverage Azure's resources still vary. However, some solutions already offer features that organizations may find appealing. These include:

1. **All-inclusive, subscription-based pricing.** A few solutions already model their backup pricing structure after Azure's pay-as-you go model. While each one's pricing structure varies, those that do offer it calculate their pricing based upon some mix of variables. Organizations should minimally expect to pay monthly based upon how much data they backup and how many VMs they protect. They may pay extra for services such as disaster recovery and premium levels of support.
2. **Policy driven backup scheduling and data placement.** SaaS-based Azure cloud backup offerings handle many mundane backup tasks, to include applying backup software fixes, patches, and upgrades. However, a few solutions support the creation of very robust backup policies. Guided by these policies, the backup software sets backup schedules for applications and dynamically changes them as needed. For instance, the backup software may change where it stores backup data or the frequency of backups to optimize them for cost or faster recoveries.
3. **Microsoft Active Directory (AD) integration.** More enterprises want to give applications owners ownership over scheduling their backup and recovery jobs. A few backup solutions already support and integrate with Microsoft's AD feature. Through this integration with AD, they can use the application owners' AD logins to assign them roles in the software.
4. **Stores backup data in Azure Blob.** Microsoft Azure Blob serves as a low cost, object-based storage target on which to store backup data. Azure Blob resides in the same physical location as the applications so backups to Blob and recoveries from it may complete more quickly. After storing backups on Blob, enterprises may take advantage of its various features, to include tiering, versioning, and data immutability.

often move their existing production databases to the public cloud to capitalize on its scalable compute and storage features. As they do, organizations must still verify they can back up and recover them in the cloud. Each TOP 5 solution can protect MySQL, Oracle Database, and SAP HANA databases hosted in the Azure cloud.

- **Perform instant recoveries.** If an application goes off-line or becomes inaccessible for any reason, users want it back online as quickly as possible. Each TOP 5 solution comes equipped to perform instant application or data restores to keep downtime to a minimum.
- **Protect on-premises data.** Many organizations adopting the Azure cloud often have applications and data residing on-premises. Any of these TOP 5 solutions can protect applications and data residing in the Azure cloud and on-premises.

- **Protect VMware applications running in Azure.** Many enterprises already run VMware on-premises and expect to continue to use it as they move into public clouds such as Azure. Each TOP 5 solution gives enterprises the flexibility to protect their VMware applications running in Azure.

All TOP 5 solutions also support the following traits:

- Backup and restore individual VMs at the file, folder, volume, and VM image levels
- Encrypt data at-rest and in-flight
- Enterprise levels of support
- Generate alerts on backup job errors and failures
- Index protected data
- May perform snapshots as frequently as once an hour
- Perform cloud-to-cloud (C2C) and virtual-to-virtual (V2V) recoveries
- Perform full and incremental backups

Differences between the TOP 5 Azure Cloud Backup Solutions

The TOP 5 solutions differ significantly in the breadth and depth of their feature support. They vary in how they protect applications and data the Azure cloud in at least the following four ways:

- **Deployment options in the Azure cloud.** Each of these TOP 5 offers different options to deploy its solution in the Azure cloud. Two make their solution as an Azure cloud-native SaaS offering. Two deliver their software as a SaaS-based offering outside of the Azure cloud. Four make their software available as an Azure virtual appliance or as software organizations may host on an Azure VM.
- **Backup storage.** Every organization should confirm the Azure storage options each TOP 5 solution offers aligns with their requirements. While they all support Azure Blob, each one manages Azure Managed Disks, Azure Files, and Azure Blob storage tiers and regions differently. The use of these tiers potentially impacts backup costs and application and data recovery times.
- **Protection of Azure applications.** The TOP 5 solutions each differ significantly in their protection of general and specialized Azure applications. Organizations might expect them to protect applications such as Azure Active Directory, Exchange, and SQL Server on Virtual Machines. Four TOP 5 solutions protect those three applications. However, only two solutions currently protect SharePoint with three offering protection for Azure Kubernetes Service (AKS). Organizations using other specialized Azure applications such as AutoScale, Container Instances, or Function must choose even more carefully. Only one solution offers comprehensive support for these specific Azure applications.
- **Protection of Azure databases.** Organizations needing to protect databases such as Azure Database for MariaDB, MySQL, or PostgreSQL, among others, will find limited choices. Only three TOP 5 solutions protect Azure Database for MariaDB or MySQL while two protect Azure Database for PostgreSQL and Azure SQL database.

TOP 5 Azure Cloud Backup Solution Profiles

Each of the TOP 5 Azure Cloud Backup Solution profiles highlights at least three ways each one differentiates itself. These differentiators represent some of the best methods that backup solutions offer to back up and recover data in the Azure cloud. Within each solution, enterprises will find distinguishing features that may better meet their respective needs.

Zerto IT Resilience Platform

The Zerto IT Resilience Platform debuts with a TOP 5 ranking in the inaugural DCIG TOP 5 Azure Cloud Backup Solutions report. Zerto recently expanded its offering to deliver backup alongside its disaster recovery (DR) capabilities. This combination gives organizations a powerful solution to which they can turn to meet their backup and recovery needs in the Azure cloud. Features that the Zerto IT Resilience Platform offers that help differentiate it from other TOP 5 solutions include:

- **Only creates compute instances in Azure needed for DR during a recovery.** Controlling costs represents one of the larger challenges that organizations face if implementing DR in the Azure cloud. Zerto helps mitigate those costs by only creating compute instances in Azure during a recovery. In the interim, organizations only incur costs for the Blob storage they use in other Azure regions. Should the need to perform a recovery arise, Zerto creates the compute instances needed for the duration of the recovery.
- **Facilitates replication and failover of VMware-based workloads.** Organizations running VMware on-premises often want to also run VMware in public clouds, to include Microsoft Azure. Microsoft's Azure VMware Solution (AVS) facilitates the introduction of VMware into the Azure cloud running on dedicated hardware. Using Zerto, organizations may replicate and move VMware-based applications and data to Azure and back again, if needed.
- **Orchestrates cohesive recoveries in Azure.** Recovering individual applications or data in the Azure cloud represents one component of a comprehensive DR strategy. Bringing up all applications at the right time to create a cohesive recovery point presents a greater challenge. Using Zerto, organizations may create consistency groups that replicate, migrate, and recover all VMs in the right order. Zerto accomplishes this feat using continuous replication and journal-based recoveries to coordinate recoveries and eliminate gaps in the data recovery.

Cobalt Iron Compass

Regardless of the public cloud in which Cobalt Iron Compass finds itself, it excels at delivering backup and recovery. Cobalt Iron completes a trifecta by earning a third TOP 5 ranking in this latest DCIG TOP 5 Azure Cloud Backup Solutions report. Organizations may deploy Compass in multiple ways in Azure and still access all its features through its all-inclusive licensing option. The features that Cobalt Iron offers that help differentiate itself from other TOP 5 Azure cloud backup solutions include:

- **Creates a cloud-like, SaaS-based backup experience across hybrid environments.** Cobalt Iron offers organizations the option to deploy Compass on physical, virtual, or cloud instances. These instance types interact with one another to function as a single,

logical converged infrastructure across physical, virtual, and cloud. Architected this way, Compass' Accelerator OS self-manages these instances to include performing ongoing software maintenance and updates. This free organizations to focus on scheduling and managing backups and recoveries.

- **Analytics engine to improve backup and recovery.** Cobalt Iron grants every Compass user access to its analytics engine. This software constantly evaluates how Compass backups perform across all enterprise environments, to include their backups in the Azure cloud. Using this information, it may then automatically act. These actions may include optimizing when backups run, resolving backup storage issues, and monitoring the infrastructure for the presence of ransomware.
- **Supports backup across multiple public and private cloud.** Cobalt Iron differentiates itself from almost all other backup solution by offering backups in multiple public and private clouds. Others generally support at most one or two public clouds in addition to providing backup for on-premises applications. In addition to Azure, Cobalt Iron Compass also protect applications and data hosted in the Alibaba Cloud, AWS, Google Cloud, and the IBM Cloud. Since many enterprises have multi-cloud strategies, they may use Compass to backup applications across all of them.

Commvault Backup and Recovery

Commvault Backup and Recovery demonstrates its ability to meet evolving organizational backup needs. As organizations adopt the Azure cloud, they may turn to Commvault to protect the applications and data they host in it. They will also find Commvault offers multiple options to protect Azure applications and databases. Commvault offers the following features that help distinguish it from other Azure backup solutions.

- **Automated spin-up and shutdown of Commvault MediaAgents.** Commvault uses VM instances in the Azure cloud to host MediaAgents with each of these instances incurring hourly costs. Commvault monitors current and scheduled backup and recovery activity on Azure. Should Commvault not need these MediaAgent instances, it shuts them down until they are needed. This helps to reduce the compute costs incurred by Commvault.
- **Compresses and deduplicates data stored on Azure Blob storage.** While all TOP 5 solutions can store backups on Azure Blob storage, Commvault also compresses and deduplicates stored backup data. Taking these extra data reduction steps helps organizations further reduce their monthly, recurring storage costs.
- **Integrates with Azure Data Box.** Organizations looking to move their existing backup stores to the Azure cloud may have large amounts of data. Organizations may use Commvault to move this data to the Azure cloud using Azure Data Box. Commvault will first move an organization's on-premises data to an Azure Data Box sent to its site. Once moved, the Azure Data Box is sent back to Azure where Commvault recovers the data onto Azure Blob storage.
- **Multiple backup management options.** Different size organizations have different backup management requirements. Some prefer to use the default backup console included with the backup software. Others prefer to use an interface offered by the cloud provider or even by a third party. Commvault supports all these management interfaces to equip organizations to manage backup in a manner that best aligns with their requirements.

HYCU for Azure

HYCU for Azure's cloud-native architecture and subscription-based pricing model represent only two of the reasons behind its TOP 5 ranking. HYCU for Azure seamlessly handles in the background all the little, hidden tasks that frequently get overlooked when performing backups. In so doing, it frees organizations to focus on why they initially Azure: to increase productivity and drive down costs. HYCU for Azure offers the following features that help distinguish it from other TOP 5 offerings:

- **Automatically optimizes backup data placement.** HYCU abstracts away the need for organizations to manage Azure Blob storage or decide between its storage tiers. It automatically places data on the most appropriate Azure Blob storage tier. Using each backup job's policies, HYCU places and retains data on different storage tiers to optimize storage costs.
- **Incurs no performance overhead on VMs when performing backups.** Like many other Azure cloud backup solutions, HYCU makes a copy of a VM by taking a snapshot of it. Once taken, HYCU differs by then reading from that snapshot copy of the VM. Taking this approach frees HYCU to use its own computing resources to back up the VM and index its data. This helps HYCU negate any possible performance impact to active applications.
- **Facilitates immediate implementation of backup jobs.** Organizations starting out with backing up their VMs in the Azure cloud may want to do it quickly and without hassle. HYCU for Azure meets these needs by offering four different default backup policies. Once subscribed to HYCU for Azure, organizations may immediately start doing backups without allocating Blob storage or creating backup policies. Organizations may also configure HYCU to automatically assign backup policies to VMs based on resource tagging.

Unitrends Backup

Unitrends Backup builds upon its success in on-premises backup to deliver a robust solution for Azure cloud backup. Previously identified as a DCIG TOP 5 all-in-one disaster recovery solutions, Unitrends continues to bring those strengths to bear. Unitrends Backup distinguishes itself from other Azure cloud backup solutions in the following ways:

- **Recovery assurance.** Unitrends stands apart as one of the only providers to formally offer backup testing and verification. Recovery assurance grants organizations the flexibility to regularly test and verify they can successfully recover from their backups.
- **Certified recoveries in the Unitrends Cloud.** Recovering applications in the Unitrends cloud serves another important purpose: organizations can certify their recoveries work. Unitrends can perform recoveries in its cloud on the enterprise's behalf to certify application and data recoveries work. Once recovered, Unitrends provides a certification the recovery worked. Third parties such as regulatory agencies accept this certification as proof that an organization can recover from a disaster.
- **Mitigates or eliminates costs and complexity of performing recoveries in Azure.** Performing recoveries in the Unitrends cloud serves yet a third purpose. It mitigates the additional compute and storage costs and configuration overhead that performing these tasks in Azure would incur. It also gives organizations confidence they can recover outside the Azure cloud should it become unavailable, which may occur.

Azure Cloud Backup Solutions Inclusion Criteria

- Protect applications and data residing in the Microsoft Azure cloud
- Meets backup and recovery requirements of all size organizations
- Solution is shipping and available by July 1, 2020
- Information available for DCIG to make an informed, defensible decision

DCIG Disclosures

Vendors of some of the solutions covered in this DCIG TOP 5 report are or have been DCIG clients. This is not to imply that their solution was given preferential treatment in this report. In that vein, there are some important facts to keep in mind when considering the information contained in this TOP 5 report and its merit.

- No vendor paid DCIG any fee to research this topic or arrive at predetermined conclusions.
- DCIG did not guarantee any vendor that its solution would be included in this TOP 5 report.
- DCIG did not imply or guarantee that a specific solution would receive a TOP 5 designation.
- All research is based upon publicly available information, information provided by the vendor, and/or the expertise of those evaluating the information.
- DCIG conducted no hands-on testing to validate how or if the features worked as described.
- No negative inferences should be drawn against any vendor or solution not covered in this TOP 5 report.
- It is a misuse of this TOP 5 report to compare solutions included in this report against solutions not included in it. ■

About DCIG

DCIG, the Data Center Intelligence Group, empowers the information technology industry with actionable analysis. DCIG provides informed third-party analysis of various cloud, data protection, and data storage technologies. Learn more at www.dcig.com.