DCIG

Arcserve UDP 9.0 Outmuscles Today's Backup Complexity and Ransomware Challenges

By DCIG CEO & Lead Data Protection Analyst, Jerome Wendt

arcserve®
Protect what's priceless.

DCIG

PRODUCT REVIEW

Arcserve UDP 9.0 Outmuscles Today's Backup Complexity and Ransomware Challenges

No organization wants to appear weak when dealing with today's backup complexity and ransomware challenges. Yet as ransomware threats spread and backup and recovery become more complex, organizations may feel helpless in the face of them. Arcserve UDP 9.0 helps organizations outmuscle these challenges by strengthening their response to them. It provides new options for organizations to centralize, simplify, and secure their backup and recovery infrastructure in today's IT environment.

arcserve®
Protect what's priceless.

SOLUTION

Arcserve UDP 9.0

COMPANY

Arcserve
8855 Columbine Road
Suite 150
Eden Prairie, MN 55347
(844) 765-7043

arcserve.com

The dynamics of managing today's organizational IT infrastructures have changed—perhaps permanently. IT environments must still contend with the constant introduction of new features, technologies, processes, and products into them. However, they must defend themselves and fight back against the new threats that ransomware presents. Further, most IT infrastructures have become hybrid, adding to their management complexity.

Perhaps nowhere does IT infrastructure complexity become more evident than when managing backups and recoveries across multiple sites. Backup solutions must manage backup jobs, place backups on multiple storage tiers, facilitate recoveries, and protect sophisticated applications. Further, they must perform these tasks in environments that remain constantly threatened by ransomware.

Outmuscling these challenges falls to third-party backup solution providers such as Arcserve. Its latest release, Unified Data Protection (UDP) 9.0, strengthens the ability of organizations to address these issues head-on. Using Arcserve organizations may better centralize, simplify, and secure backup and recovery across their hybrid cloud environment.

Challenges and Threats Organizations Face

In managing backup and recovery in today's IT infrastructure, organizations often face the following challenges and threats:

1. ***No centralized backup console.*** IT personnel may work remotely and/or in any organization's location. However, they must manage backup and recovery tasks across virtual, physical, and cloud deployments. This creates a need for a single management console that centrally manages backup and recovery across these different locations.
2. ***Need for multiple backup administrator roles.*** Designating one individual or a dedicated team of professionals to manage backups and recoveries may not always make sense. Certain applications or workloads in organizations may require individuals with specific knowledge to best manage those backups. A backup solution that supports different administrator roles offers improved security and administration of backup and recovery tasks.
3. ***Vulnerable identities of IT personnel.*** Bad actors develop ransomware strains that target and probe IT environments for vulnerabilities. Some strains focus on compromising logins to backup solutions by identifying those individuals with weak passwords. Once compromised, these bad actors may access the solution to compromise or delete existing backups and backup jobs and/or disable new ones. Backup solutions must validate identities of individuals as they access the solution and then perform tasks once logged in.
4. ***Lack of sophisticated backup and recovery features.*** Organizations have their choice of multiple backup solutions built for their IT environments. However, today's applications often have specific and sophisticated backup and recovery needs. Unfortunately, some backup solutions may lack the robust feature set that organizations need to fully protect these applications and their data.

Arcserve UDP's Strong Foundation

Arcserve's Unified Data Protection (UDP) offers a decided edge over many competitors. UDP delivers top-rated, next-generation backup and recovery features that organizations routinely use. UDP has for years offered and supported:

- A partnership with Sophos that provides proactive response to ransomware attacks on backup data.
- Backup appliances that facilitate turnkey deployments in remote offices and data centers.
- Broad support for protecting applications and operating systems.
- Cloud-based immutable stores in AWS S3, Wasabi, and Nutanix.
- On-premises protection of Microsoft 365 using Arcserve UDP.
- Global source-side deduplication that reduces backup times and backup storage needs.
- Support for multiple backup target types (cloud storage, disk, and tape.)
- Using a validated configuration of sending backups to an on-premises Arcserve OneXafe immutable digital vault.
- Multiple methods to perform instant recovery for different application requirements.
- Cluster-like HA for applications and data using UDP's Virtual Standby feature.
- Worldwide technical support that supports UDP deployments around the globe.

UDP's use in IT environments worldwide continues to provide Arcserve with an advantage over many competitive offerings. Arcserve does not have to guess which new backup and recovery features organizations need next. Their existing deployments and ongoing customer interactions help Arcserve prioritize which features to include in UDP 9.0.

Central Cloud Console for Lockdown and Lockout

If poorly implemented, backup and recovery management in IT environments quickly becomes a tedious, laborious, and error-prone task. Managing backup across multiple locations may lead to unforeseen outcomes, even if all sites use the same management console. For instance, backup policies may be applied inconsistently or not at all due to poor oversight and coordination. These practices weaken an organization's ability to reduce complexity and mitigate ransomware threats.

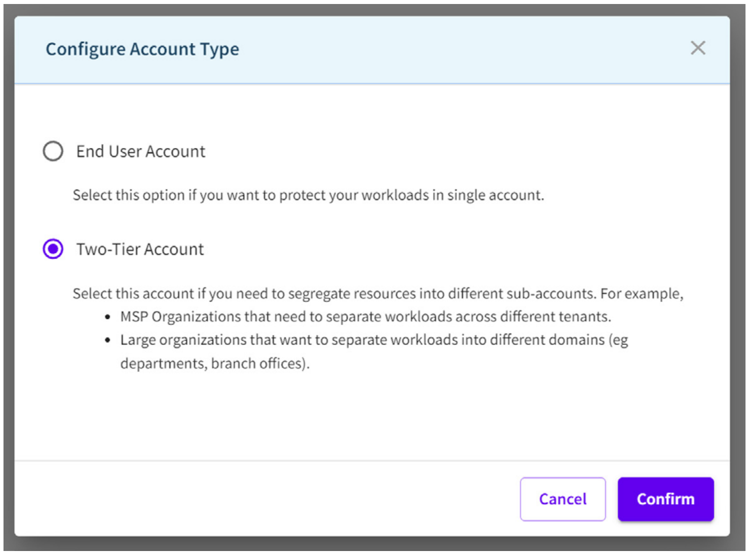
UDP 9.0's introduction of a Cloud Console strengthens an organization's response to ransomware in multiple ways. Arcserve hosts and maintains this console in a cloud data center. Delivered this way IT personnel do not have to manually deploy or install it or spend extended amounts of time configuring it. Rather, they may quickly log in and use its intuitive interface to start performing tasks that help lock down their backups. These tasks include:

- Creating and defining backup policies.
- Configuring the infrastructure, source groups, and user access controls.
- Managing account resources, to include user management.
- Monitoring and analyzing backup and recovery jobs throughout the organization.

The Cloud Console then takes steps to lock out bad actors. To secure each individual's access to the Cloud Console and organizational backups, it uses strong authentication. IT personnel must use multifactor authentication (MFA) to access the UDP Cloud Console. The UDP Cloud Console authenticates each login through its MFA integration with Okta. This MFA authentication verifies each user's identity and counters possible attacks by bad actors.

> ***"The UDP Cloud Console provides central user account management to simplify ongoing user management."***

Once logged in, the UDP Cloud Console provides central user account management to simplify ongoing user management. For instance, it offers role-based access controls (RBAC) that manage and control user activities using Arcserve Identity services. Using these controls, it assigns IT personnel either "Super" admin or tenant-level roles with responsibilities assigned to them accordingly.



Configure Account Type

○ End User Account

Select this option if you want to protect your workloads in single account.

● Two-Tier Account

Select this account if you need to segregate resources into different sub-accounts. For example,

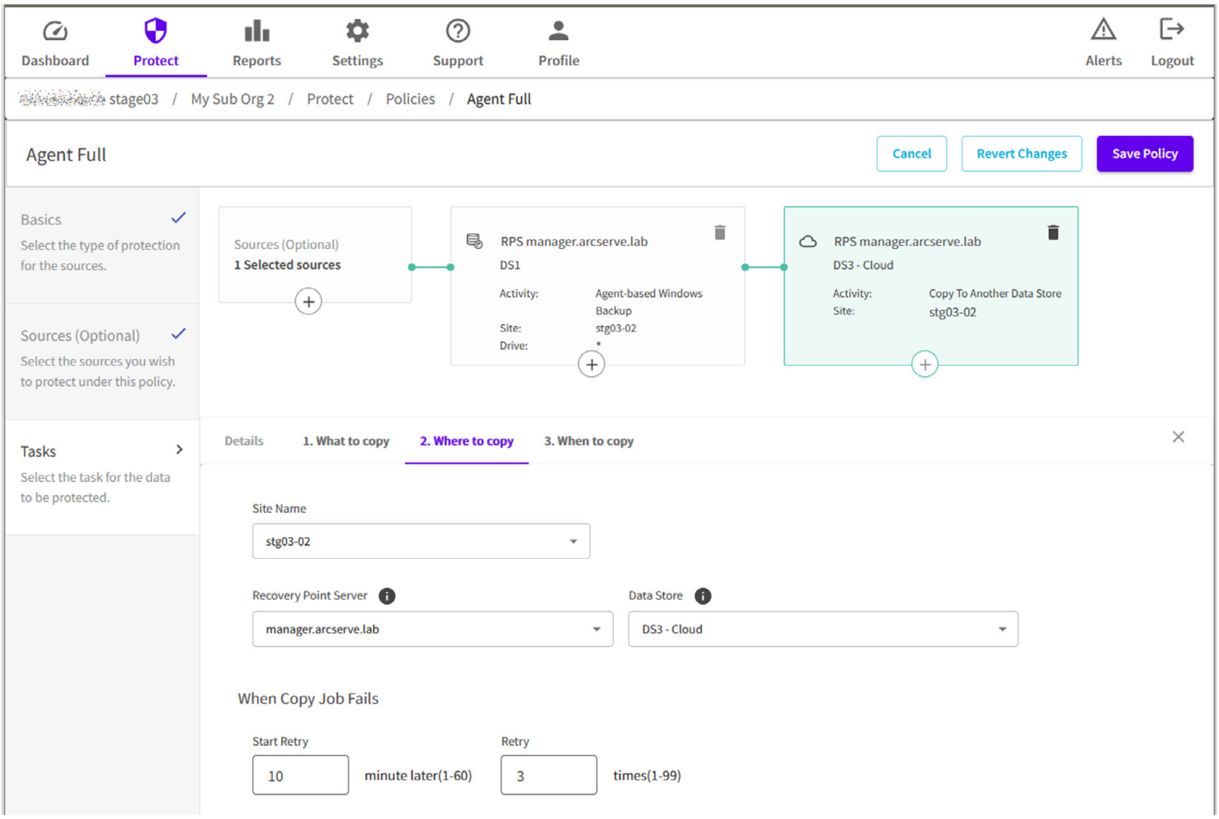
- MSP Organizations that need to separate workloads across different tenants.
- Large organizations that want to separate workloads into different domains (eg departments, branch offices).

Depending on their assigned permissions, IT personnel may manage UDP backup and recoveries at any site within an organization through its Cloud Console. The Protect tab on the Console enables them to:

- Select workloads to protect.
- Select the locations where they want to store the backups. This location may include choosing a central Arcserve Recovery Point Server (RPS) as a storage target.
- Perform restores and recoveries.

Through the UDP Cloud Console, IT personnel may also view and manage Arcserve Cloud Direct backup jobs. Arcserve Cloud Direct operates separately as a backup-as-a-service (BaaS) that Arcserve also hosts in its cloud. Cloud Direct performs on-premises backups without requiring any hardware or software installations and sends backups directly to the Arcserve cloud.

These UDP 9.0 features should result in more organizations centralizing their backup management to improve their security posture. To meet this forecast demand, Arcserve continues to provide and support an on-premises private management console that supports ten different languages. Organizations may continue using this console and then switch to the UDP Cloud Console at any time.



stage03 / My Sub Org 2 / Protect / Policies / Agent Full

Agent Full

Basics ✓
Select the type of protection for the sources.

Sources (Optional) ✓
Select the sources you wish to protect under this policy.

Tasks
Select the task for the data to be protected.

Sources (Optional)
1 Selected sources

RPS manager.arcserve.lab
DS1
Activity: Agent-based Windows Backup
Site: stg03-02
Drive: *

RPS manager.arcserve.lab
DS3 - Cloud
Activity: Copy To Another Data Store
Site: stg03-02

Site Name: stg03-02

Recovery Point Server: manager.arcserve.lab

Data Store: DS3 - Cloud

When Copy Job Fails

Start Retry: 10 minute later(1-60)

Retry: 3 times(1-99)

> ***"The Cloud Console provides response times that match what users expect if they manage UDP on-premises."***

An Empowered Cloud Backup Experience

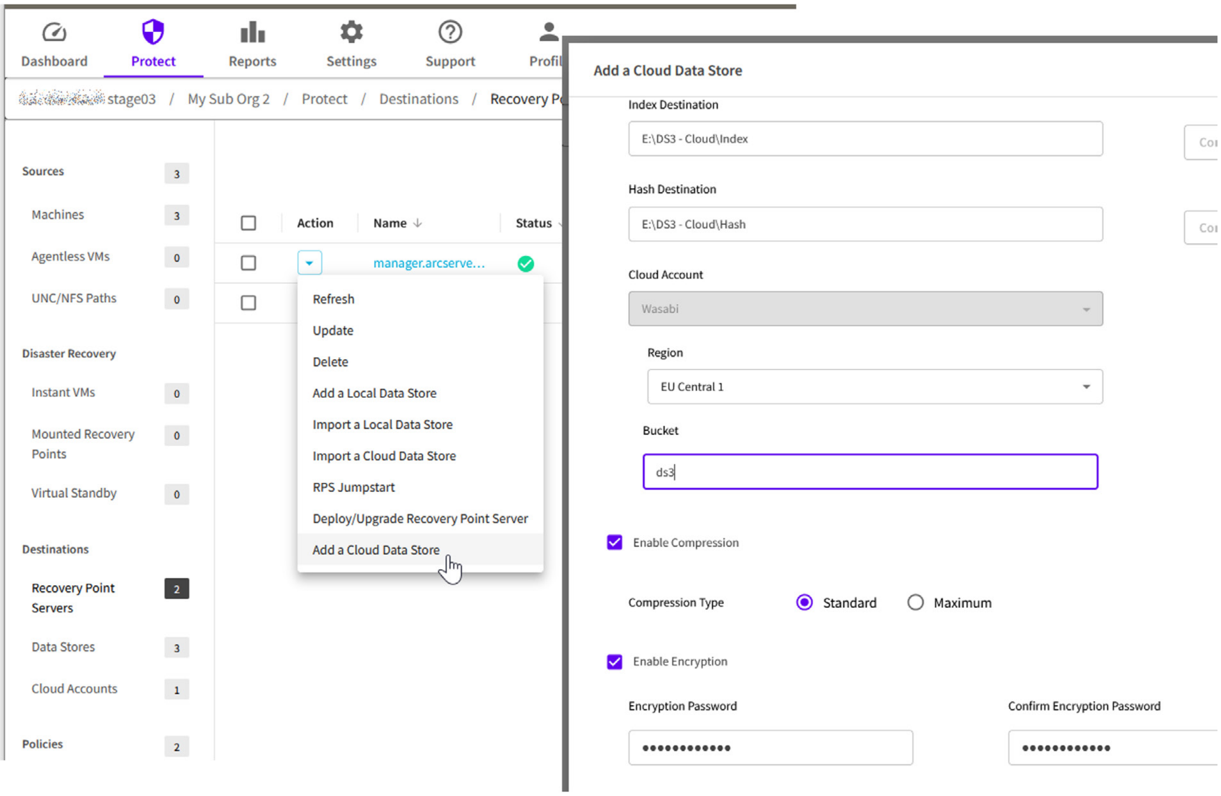
IT personnel have little patience or tolerance for slow, passive management web interfaces, especially those running in the cloud. If it runs in the cloud, they want it to run faster and better. To meet these expectations, Arcserve moved to using REST APIs. Using these APIs, the Cloud Console provides response times that match what users expect if they manage UDP on-premises.

This centralized management console empowers users in other ways by granting them faster access to new features. This already shows up in Arcserve's support of more cloud storage targets. Arcserve UDP 9.0 can directly back up to any of the following cloud object storage offerings:

- Amazon Web Services (AWS) Simple Storage Services (S3)
- Google Cloud Storage
- Wasabi Cloud Storage

Backing up to these storage targets positions organizations to capitalize on the advantages that cloud object storage provides. These benefits may include:

- Access to affordable storage capacity that may be quickly and easily added.
- High levels of availability, reliability, and resiliency.



Add a Cloud Data Store

Index Destination: E:\DS3 - Cloud\Index

Hash Destination: E:\DS3 - Cloud\Hash

Cloud Account: Wasabi

Region: EU Central 1

Bucket: ds3

☑ Enable Compression

Compression Type ● Standard ○ Maximum

☑ Enable Encryption

Encryption Password: ●●●●●●●●●●●●

Confirm Encryption Password: ●●●●●●●●●●●●

Arcserve UDP's support of more cloud object storage targets complements its support for local backups. These remain a necessity for production workloads that require fast backups, restores, and recoveries. Using local backups organizations avoid the potentially long wait times associated with retrieving data from the cloud.

"UDP 9.0 may perform granular restores of an Oracle PDB down to a specific tablespace within Oracle."

More Powerful Backup and Recovery Options

The use of leading databases, cloud platforms, hypervisors, and operating systems (OSes) by organizations has not abated. If anything, organizations use these more so they want more powerful backup and recovery features to protect them. Arcserve UDP 9.0 addresses these concerns in the following ways.

Oracle and SQL Server Data Protection

On the database side, UDP 9.0 enhances its existing data protection features for Oracle and SQL Server databases. Arcserve UDP 9.0 offers full or granular recovery for Oracle Pluggable Databases (PDBs).

Arcserve UDP has provided an agentless backup of Oracle Database through its integration with Oracle RMAN since UDP's 8.x release. UDP 9.0 builds on that integration to quickly back up and recover multiple terabytes of an Oracle PDB.

UDP 9.0 may perform granular restores of an Oracle PDB down to a specific tablespace within Oracle. This support extends to Oracle DBs running on Solaris x64 platforms. All existing features including non-disruptive testing using Assured Recovery, full DB-level restores, granular recovery, and other capabilities are available.

Arcserve also strengthened UDP 9.0's backup and recovery features for Microsoft SQL Server. It takes an extra step for SQL Server backups when performing consistency checks on them. If the consistency check fails, it generates an alert and marks the backup as unusable for restores.

UDP 9.0 offers point-in-time restores available from within the UDP UI. This permits IT personnel to restore a database to any transaction point between two recovery points using its Point-in-Time Recovery feature.

> ***"UDP 9.0 permits IT personnel to restore an SQL Server database to any transaction point between two recovery points using its Point-in-Time Recovery feature."***

Other new options UDP 9.0 offers to better protect and restore SQL Server database include:

- Increased security by restricting access to specific roles.
- Freedom to restore a SQL Server database to alternate servers, instances, and paths.
- Choice between recovery and norecovery modes.
- Proactively verifying a target SQL Server has FileStream Enabled before starting a restore.

OS Platform Support

Operating systems (OSes) do not stand still either with organizations routinely upgrading to current OS releases to ensure uninterrupted technical support. To meet these needs, Arcserve UDP 9.0 adds support for the latest Linux, Microsoft Windows, and VMware releases.

UDP 9.0 adds support for Gen 2 VMs on Microsoft Azure when using Virtual Standby (VSB).

Virtual Standby offers cluster-like high availability (HA) for applications and data. It can also rapidly convert the recovery points (backups) to a wide range of VM formats.

Organizations may use these recovery points to automatically, or manually, power on a VM. Virtual Standby supports VMs hosted in multiple private and public cloud platforms that include Amazon EC2, Microsoft Azure and Hyper-V, Nutanix AHV, and VMware vSphere.

Arcserve UPD 9.0 Support for Database and Operating System Platforms

Arcserve UDP 9.0 supports the latest versions of the following databases, hypervisors, and operating systems.

Platform	Release
Databases	· Oracle 19c and 21c Stand-alone on Oracle Solaris 11.x (x64) · Oracle Database 21c
Hypervisors	· VMware vSphere 7.0 Update 3 · VMware vSphere 8.0
Linux	· AlmaLinux 8.4, 8.5, 8.6, 9.0 · Debian 9 – 11 · Oracle Linux 8.4, 8.5, 8.6, 9.0 · Red Hat Enterprise Linux 8.x, 9.x · Rocky Linux 8.4, 8.5, 8.6, 9.0 · SLES 15 SP3, SP4 · Ubuntu 22.04 LTS
Windows	· Microsoft Windows 11 · Microsoft Windows Server 2022

UDP's Multiple Backup and DR Capabilities

Arcserve UDP has for some time delivered advanced data protection features at its core that organizations routinely use. Arcserve offers both agent-based and agentless backup options. These give organizations the flexibility to use the best backup approach to meet specific application data protection requirements.

On the recovery side, Arcserve UDP offers multiple disaster recovery (DR) options that include:

- ***DRaaS.*** Arcserve UDP offers comprehensive data protection with on-premises and cloud-based deployments. DRaaS is available via its fully managed cloud services extension known as Cloud Hybrid. Its DRaaS service keeps critical data and workloads protected offsite and available and positions organizations to continue operations during or after unplanned on-premises outages.
- ***Instant Restores.*** Using its Instant Restore feature, IT personnel may quickly spin up a VM directly out of a backup. They can recover a VM without first needing to recover or rehydrate the backup.
- ***Virtual Standby (VSB).*** Offers a highly available configuration for data and applications for even faster recoveries than its Instant Restore feature. VSB creates and maintains a VM with a recovery point that is ready to boot at any time. Once configured, VSB constantly monitors the heartbeat of the source (production) node. Should it detect that the source node fails or goes off-line, the VM immediately takes over as the primary node.

Arcserve UDP 9.0 Outmuscles Today's Backup Complexity and Ransomware Threats

No organization can respond to today's backup complexity and ransomware threats with a weak backup solution. They need a backup solution that outmuscles them. It must strengthen their security posture while equipping them to protect more complex IT environments.

Arcserve UDP 9.0 provides the powerful response that today's organizations expect and need by:

- Delivering a new cloud-based, multi-tenant Cloud Console that centrally manages UDP and Cloud Direct.
- Enhancing its protection of enterprise applications like Oracle and MS SQL Server.
- Making architectural and user interface enhancements to improve performance and simplify management.
- Improved resilience, availability, and durability for data through its support for multiple cloud object storage providers.

These features combined with Arcserve's existing integration with Sophos provide organizations with a reinforced beachhead against ransomware threats. As it defends against ransomware's threat, it simultaneously provides more powerful and easier to use data protection capabilities. Using Arcserve UDP 9.0 organizations empower themselves to defend against the latest ransomware threats and overcome the complexity inherent in IT environments. ■

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. More information is available at **www.dcig.com.**