KuppingerCole Report

EXECUTIVE VIEW

By Mike Small

July 19, 2022

Arcserve Unified Data Resilience

Data resilience solutions are an essential element of business continuity plans and, as organizations go through digital transformation and become more dependent upon their IT services, the need for data resilience has grown. These solutions must not only support today's hybrid multi-cloud IT service delivery environment, but also exploit the new capabilities that this provides. This report covers how the data resilience solutions provided by Arcserve meet these challenges.

By **Mike Small**

sm@kuppingercole.com

Content

1 Introduction

As organizations go through digital transformation, they become much more dependent upon their IT services to support the business, and this has increased the potential business impact of accidental mistakes, natural disasters, and cyber incidents. This makes business continuity planning an essential element in the digital transformation process. The use of data resilience solutions and disaster recovery services are essential elements of business continuity plans, and these must support today's multi-cloud hybrid IT environment.

Data is the most important business asset of the modern enterprise and needs to be protected against unwanted events such as malware as well as physical or logical damage to the storage devices or the IT installation. The prevalence of ransomware attacks where criminals demand payment to restore access to business-critical data has emphasized the need for data resilience. In addition, the changes in working patterns following the COVID-19 pandemic have also increased the risks to data as people work from home. As well as increasing susceptibility to ransomware, unmanaged end user equipment often lacks proper data protection.

When IT services were delivered exclusively on-premises, backup solutions were used to make copies of the data storage media (typically tape and disk) which were then stored in separate locations with additional safeguards against fire and theft. The physical transfer of these media added delays and additional risks into the backup and recovery processes. However, IT services are now delivered through a hybrid model which introduces new challenges and provides new opportunities.

In today's hybrid multi-cloud IT environment, some services remain on-premises while others are delivered through the cloud. There is a temptation to believe that the use of a cloud service removes the need for the customer to consider the resilience of their data. The responsibility for data held in cloud services is shared between the tenant and the service provider and there are many situations where the tenant is responsible for the resilience of their data. In addition, where the hybrid model leads to multiple data protection solutions being used, which increases the management burden. Therefore, it is especially important to implement a single solution that covers all the different use cases.

The cloud also provides an alternative location for backed-up data since major cloud services are usually delivered from highly secured datacentres in multiple geographic locations. This provides the possibility to store the backed-up data with a high degree of resilience as well as reducing the delays and risks of physical transfers. Modern data resilience solutions can be expected to offer backup to the cloud as an option.

The time criticality of digitized business services has increased the need for an always on architecture. Today's e-commerce, financial services, and critical infrastructure demand continuous availability where even seconds of downtime could lead to severe damage. This always on architecture depends upon

continuous data replication to ensure business continuity when individual elements fail.

All organizations need to consider the risks related to the availability of their business data and respond appropriately to mitigate these risks. This means investing in backup products, disaster recovery services and immutable storage solutions to ensure data resilience. It is vital that the chosen approach is adequate for the modern digitally transformed hybrid IT environment.

2 Product Description

Arcserve is a global company with headquarters in Minneapolis, Minnesota in the USA. It was founded in 1983 as Cheyenne Software Inc and launched Cheyenne NetBack in 1988. The Original Arcserve product was released 2 years later in 1990. It was then acquired by CA Technologies in 1996 and in 2014 became a private company under the ownership of Marlin Equity Partners. In March 2021, Arcserve announced the completion of its merger with StorageCraft.

Arcserve provides a complete range of data resilience solutions that provide comprehensive data protection, data management, and disaster recovery capabilities. These cover the business continuity challenges for organizations of varied sizes from SMB to large enterprises. They help to manage and protect critical business data across systems and applications, both on-premises or in the cloud.

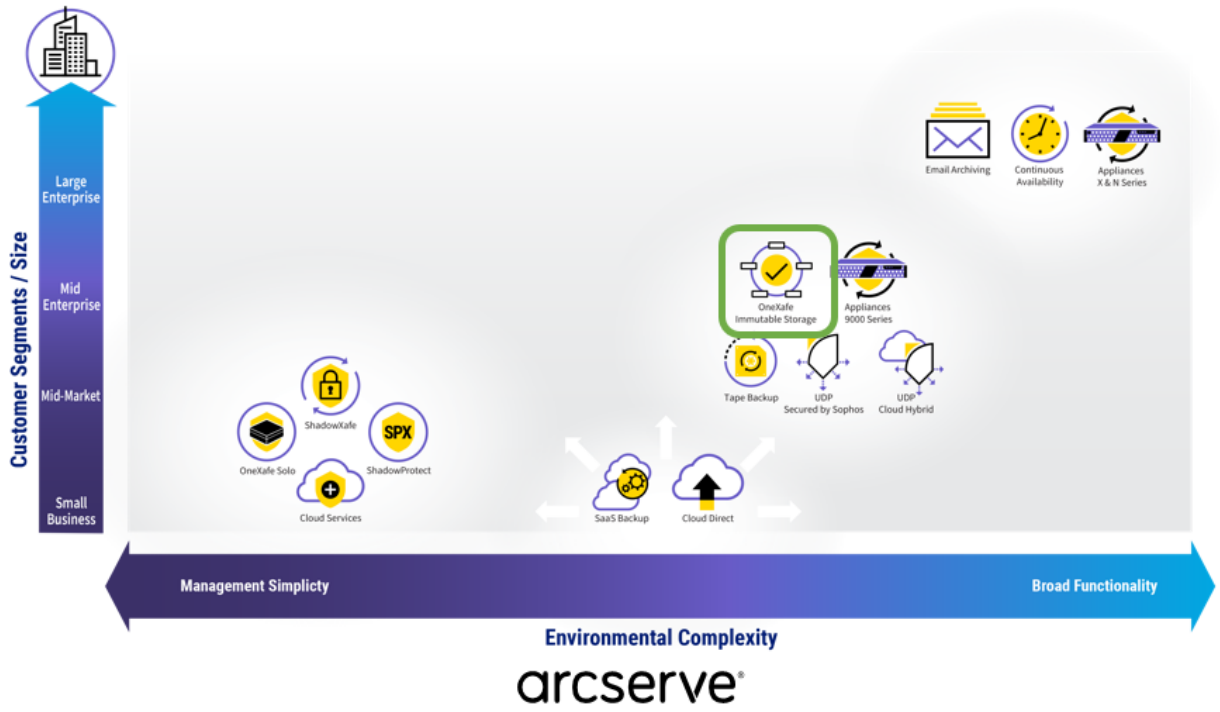

Figure 1: Arcserve Unified Data Resilience Platform (source Arcserve)

The solutions include software products, hardware appliances, and cloud-based services.

Arcserve Unified Data Protection (UDP) 8.1. This is the Arcserve's lead data protection product. It supports hybrid business continuity topologies, including local backup and multiple sites, as well as cloud services

and backup to cloud. It enables backup to either a local machine or a central recovery point server (RPS) with global, source-side deduplication. It includes integration with Sophos Intercept X Advanced for Server, providing protection against ransomware and a wide range of cyber threats. This solution targets midmarket and enterprise customers.

Arcserve Backup. This is a storage management solution for distributed and multiplatform environments that can backup and restore data from every machine on a network, including those running Windows, UNIX, and Linux. It offers complete control and visibility from one management console across different platforms and organizations. This solution targets midmarket and enterprise customers.

Arcserve Continuous Availability. This is a data replication solution that synchronizes the data on Windows and Linux systems with a second physical or virtual system locally, at a remote location, or in the cloud. Once synchronized, byte-level changes are continuously replicated. This helps to ensure business continuity for critical applications and systems. This solution targets midmarket and enterprise customers.

In addition, Arcserve offers a range of hardware appliances. These combine flash-accelerated deduplicated storage and high-speed networking with threat prevention technologies, highly redundant hardware and cloud services for plug-and-play backup, security, DR, and application availability. The appliances include integration with Sophos Intercept X Advanced for Server, providing server protection against ransomware and a wide range of cyber threats.

Arcserve OneXafe is a scale-out object-based NAS appliance with built in enterprise-grade features such as immutable snapshots, inline deduplication, encryption at rest, and disaster recovery with WAN optimised replication. OneXafe's file system provides an immutable object store, with every object written only once and never modified. Any modification made to the file system always results in the creation of new objects. OneXafe continuous data protection (CDP) takes snapshots every 90 seconds. These cannot be changed or modified by an external source and make it possible to go back to specific points in time and recover entire file systems.

2.1 Key Capabilities

At KuppingerCole, we look for the certain key capabilities in data resilience and disaster recovery solutions. The following paragraphs describe how Arcserve data resilience products provide these capabilities.

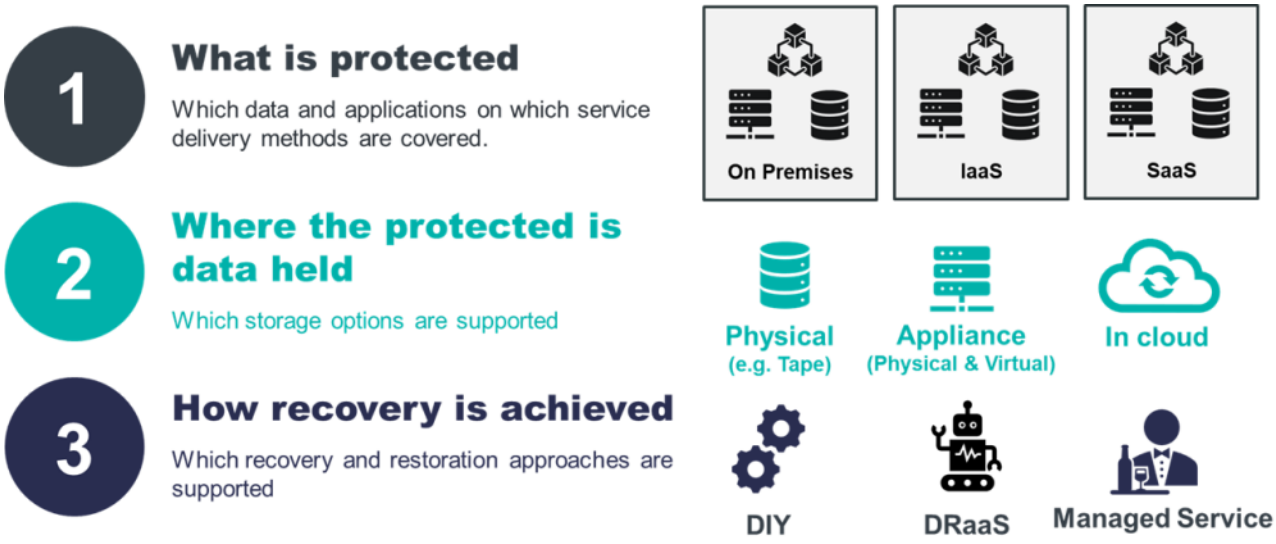

Figure 2: Key Capabilities of Data Resilience and Disaster Recovery

Protected Data - The solution should support the wide range of data types commonly found in organizations including unstructured data in all its various forms, files systems, and databases. As well as the traditional relational databases, the NoSQL types of databases relevant for big data and data analytics that are increasingly important to digital transformation should be covered. It should also support snapshots of physical servers, VMs, cloud VMs and containers to enable rapid service restoration.

Arcserve data resilience solutions protect Nutanix Hyperconverged Infrastructure with Nutanix AHV, Files and Objects integration, as well as VMware, Hyper-V, RHEV, KVM, Citrix, and Xen VMs with a selection of agentless and agent-based backups.

They provide backup and recovery for Oracle Databases with native RMAN integration, as well as Microsoft SQL Server (including FCI clusters), Exchange, SharePoint, Active Directory, and Microsoft 365. They also provide protection for File Servers, NAS, SAN, UNIX, FreeBSD, AIX, HP-UX, Solaris, SAP R/3, SAP HANA, and more, as well as shielding them from ransomware.

IaaS Protection - Many business-critical applications are now deployed on IaaS and, while the CSP (Cloud Service Provider) is responsible for the infrastructure, the customer is responsible for the resilience of their data. The solution should provide protection for applications and data held in commonly used IaaS cloud services.

Arcserve UDP agent for Windows can be deployed on Amazon EC2 VMs. It provides protection for all the OS/Applications supported by physical machines that are supported as Virtual Machines on AWS EC2. It can also be deployed on Azure with the same capabilities.

Arcserve supports BMR for backups into Azure where the source can be Physical, or Virtual and regardless of the original Hypervisor. This restore method uses the VSB (Virtual Stand By) mechanism. The same is also supported for AWS but requires a Proxy machine running in AWS.

SaaS Protection - Organizations are now using business applications delivered via SaaS and, while the CSP is responsible for providing some level of service continuity, this may not meet the business requirements of the customer organization. For example, the RTO (Recovery Time Objective) may be too long or there may be inadequate protection against customer errors. The solution should provide protection for the data held in SaaS services, including the commonly used office productivity tools and CRM systems, and cover the variety of data types held within these. It should also support custom retention schemes.

Arcserve has 2 offerings for this: Arcserve SaaS Backup offers complete cloud-to-cloud backup for data stored in Microsoft 365, Microsoft 365 Azure AD, Microsoft Dynamics 365, Salesforce, and Google Workspace. Arcserve Unified Data Protection and Appliances deliver comprehensive on-premises protection for Microsoft Office 365, including Exchange Online, SharePoint Online and OneDrive for Business

Choice of storage - The customer should have a choice of how and where the protected data is stored. Backup solutions often work by writing the protected data to disk or tape library devices. The cloud-based solution should provide compatibility so that it works seamlessly across different protected environments. It is also important to provide a route to move the backed-up data out of the cloud service should this be needed. The customer should be able to choose the cloud service used and to ensure that their data is stored within their chosen geographical regions.

Arcserve UDP integrates on and off-site backup and restore with built-in cloud DR and backup to the Arcserve® Cloud, as well as to private and public clouds, including Amazon® AWS, Microsoft Azure®, Oracle Cloud®, Nutanix® Objects, and others. The customer can choose the geographic location of where their protected data is held using the capabilities provided by the cloud service.

For on-premises storage, Arcserve offers OneXafe, an immutable object-based network-attached storage (NAS) solution with a scale-out architecture, which allows the user to add one drive at a time or multiple nodes in a cluster. OneXafe provides immutable and scale-out storage for large-amount of unstructured data and vendor agnostic backup targets. This avoids the need to allocate extraneous storage capacity to compensate for scale-up storage architectures. It combines the advantages of a distributed, immutable object-store with the accessibility of SMB and NFS protocols. It includes enterprise features such as global inline deduplication, compression, CDP, and encryption at rest as well as Immutable data protection snapshots.

Security - The solution should ensure that the data in transit to and from the backup location is secured against unauthorized access, leakage, and eavesdropping. The backed-up data at rest should be protected against unauthorized access and disclosure by the solution provider, the cloud service provider, and other parties. It should support strong certified encryption technologies where the customer controls the keys. It should also enable role-based access control over the administrative functions, and support for MFA authentication should be provided.

The Arcserve products include a wide range of security features. Arcserve UDP supports Role Based Administration to limit the scope for administrative misuse and mistakes. It provides encryption of protected data in flight using TLS 1.2 and at rest with AES-256. The data is encrypted on the protected server before being sent to the backup destination. Backups held within AWS can be protected against deletion or

alteration with immutable cloud storage using the AWS S3 Object Lock. Integration with Sophos Intercept X Advanced for Server protects the UDP recovery point servers (RPS) and the management console against a wide range of cyber threats.

Arcserve OneXafe immutable storage provides strong protection against ransomware as data is never overwritten when being updated and can easily be restored back to an earlier copy. It uses a mathematical system similar to that used on blockchains to protect the stored data against unauthorised changes and deterioration (sometimes called bit rot). Its architecture is designed to support 90 second snapshots and rapid restoration of data when this is required.

Disaster Recovery - The solution should provide the capability for disaster recovery. The range of DRaaS services covered should include:

- A fully managed service covering all aspects.
- Assisted recovery, where the offering provides the recovery infrastructure and manages data replication.
- Self-service where the solution provides the tools needed to accomplish the various tasks.

Arcserve Cloud Hybrid DRaaS provides failover capabilities for on-premises servers by transferring images to the Arcserve Cloud Hybrid datacentres. In the event of a disaster, these backup images are used to run virtual instances of the servers in the Arcserve Cloud Hybrid infrastructure. Users can access these via secure virtual private network (VPN) connectivity.

UDP Virtual Standby enables the customer to maintain virtual copies of systems on Nutanix AHV, VMware vSphere, Microsoft Hyper-V, Amazon AWS EC2, and Microsoft Azure. UDP Instant VM allows Ad-Hoc spin up of backups as virtual machines on the local backup server or any VMWare or Hyper-V host

Arcserve Live Migration automatically synchronizes files, databases, and applications on Windows and Linux systems with a second physical or virtual environment located on-premises, at a remote location, or in the cloud. Once synchronized, changes are replicated in real time to ensure the source and target are in sync prior to the migration. Arcserve Live Migration orchestrates the cutover to the target destination to take the complexity out of the migration.

3 Strengths and Challenges

Arcserve has a mature set of data resilience solutions with a strong user base. These solutions provide comprehensive capabilities that can satisfy many use cases across organizations of different sizes from SMBs to large enterprises. The addition of the OneXafe storage appliances from StorageCraft strengthen these capabilities, providing increased flexibility, energy efficiency as well as added security.

The solutions can be deployed as software, hardware, and virtual appliances, as well as within cloud services. The solutions support agentless protection of VMware, Hyper-V and Nutanix deployments. They provide integrated automatic deduplication of the protected data and support a choice of storage options including traditional tape backup as well as cloud. The solutions also offer resilience for data deployed in both IaaS and SaaS, covering the major hyperscale clouds and Microsoft 365.

The Arcserve unified data resilience solutions provide very strong capabilities to secure the protected data against unauthorized access as well as from hardware failures human errors and cyber-attacks. These include capabilities to encrypt the protected data before it leaves the customer, together with immutable storage to protect the data against malicious changes. They are also integrated with Sophos X to provide protection against a wide range of cyber-threats.

Strengths

- Mature product with strong user base.
- Comprehensive functionality covers multiple use cases.
- Agentless VMware and Hyper-V and Nutanix protection.
- Integrated source side global deduplication.
- OneXafe provides a distributed, immutable object-store using standard storage protocols.
- OneXafe is highly energy efficient supporting sustainable computing.
- Wide choice of cloud service providers for backup storage and disaster recovery.
- Arcserve UDP and Appliances protect Microsoft 365 data on premises, in addition to other workloads.
- Arcserve SaaS Backup offers complete protection for data stored in Microsoft 365, Microsoft 365 Azure AD, Microsoft Dynamics 365, Salesforce, and Google Workspace.
- Exploits AWS S3 Object lock to provide backup immutability.
- Integration with Sophos Intercept X provides protection against cyber threats.

Challenges

- Integration of the business and technology with StorageCraft.
- UDP Backup to cloud requires an on-premises server.
- Limited integration with snapshot capabilities for major cloud services.
- No inbuilt functionality to detect sensitive data in backups.
- Does not support eDiscovery searching
- Does not support tiered long-term retention capabilities.

4 Related Research

Market Compass Cloud Backup and Disaster Recovery
Buyers Compass Hybrid Cloud Backup and Disaster Recovery
Market Compass Global IaaS Providers Tenant Security Controls
Leadership Compass: Endpoint Protection Detection & Response
Leadership Brief: Incident Response Management

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.