KuppingerCole Report

MARKET COMPASS

By Mike Small
January 18, 2022

Cloud Backup and Disaster Recovery

The KuppingerCole Market Compass provides an overview of the product or service offerings in a certain market segment. This Market Compass covers solutions that provide backup, restore and disaster recovery of IT service data into the cloud in the context of the hybrid IT service delivery environment that is now commonly found in medium to large organizations.

By **Mike Small**
sm@kuppingercole.com

Disclaimer: This is an abridged version of the KuppingerCole Report Market Compass for Arcserve. The full report contains further Product/Service descriptions from other vendors under item 5.

Content

1 Management Summary

The KuppingerCole Market Compass provides an overview of a market segment and the vendors in that segment. It covers the trends that are influencing that market segment, how it is further divided, and the essential capabilities required of solutions. It also provides ratings of how well these solutions meet our expectations.

This Market Compass covers solutions that...

provide backup, restore, and disaster recovery of all data held in IT services into the cloud in the context of the hybrid IT service delivery environment that is now commonly found in medium to large organizations. It provides an assessment of the capabilities of these solutions to meet the backup and disaster recovery needs of organizations with a complex hybrid IT delivery environment.

There is a mature market with many existing backup and disaster recovery solutions that support the protection of data in IT services delivered on premises by backing up data to physical media. However, the way in which IT services are delivered is changing as organizations move to a hybrid delivery model. This is leading to emerging markets for solutions that protect data in SaaS (Software as a Service) and IaaS (infrastructure as a Service) as well as for solutions that use cloud services to secure the backed-up data. There is also an emerging market to offer enterprise backup and DR as software as a service.

The changes in working patterns caused by the COVID-19 pandemic have also led to increased risks as people work from home. These risks include increased susceptibility to ransomware through the use of unmanaged end user equipment as well as a lack of data protection for these devices.

Most of the existing vendors are adapting their solutions to this new model, but most still have some way to go, especially around SaaS platforms. In addition, new vendors, including the cloud service providers themselves, are offering solutions covering their cloud as well as for storing data from on premises and other clouds. For SaaS, most vendors now offer solutions for customers to back-up the data held, especially for Microsoft 365. A few also offer solutions that cover Google Workplace and Salesforce, however, there is a lack of comprehensive coverage for other data in other SaaS platforms.

The essential capabilities that customers should look for in solutions must be aligned with their business requirements for service continuity. This includes considering how business critical the various systems and data are, and hence, the protection that is needed (recovery objectives). In general, where an organization is already using an existing solution for on-premises protection, this will be preferred over adding other solutions, providing it meets their evolving business needs. Adding new solutions increases not only costs but also adds to the complexity of use and maintenance. However, in our research we see that some existing solutions on the market do not yet provide comprehensive coverage for the hybrid IT model. Where an existing solution does not meet the business requirements, the organization should consider the new to market solutions, if only as a stop gap.

Highlights:

- This report covers solutions that provide backup, restore, and disaster recovery of IT service data into the cloud in the context of the hybrid IT service delivery environment.
- Ensuring the continuity of IT services is an essential part of the security triad of confidentiality, integrity, and availability.
- The increasing business dependence on IT services through digital transformation, together with prevalence of ransomware, make backup and disaster recovery an essential for organizations.
- There is a mature market with many existing backup and disaster recovery solutions that support the protection of data in IT services delivered on premises by backing up data to physical media.
- This model is now changing as organizations are now using a mixture of on premises and cloud delivered services. In addition, the cloud services are useful to provide longer term storage for backed-up data and disaster recovery capabilities.
- There are also benefits from delivering backup and disaster recovery as a cloud service (e.g., DRaaS). This avoids the need to buy and maintain backup devices and infrastructure at a secondary site.
- There are several scenarios that solutions must cover. These are: on premises workloads, IaaS workloads, SaaS data, as well as disaster recovery.
- In our view, the market for protection of SaaS and IaaS will increase significantly. In addition, organizations will adopt backup and disaster recovery as a cloud service.
- In this report vendor's products are evaluated against the following capabilities: basic capabilities for backup and restore, extended capabilities, data security, compliance support, disaster recovery, SaaS support, IaaS support and on premises support. Our evaluation of these capabilities is displayed for each vendor on a spider chart.
- In addition, each vendor is evaluated against our standard criteria of Security, Deployment, Interoperability, Usability and Market standing.
- The report also identifies the vendors that in our evaluation provide noteworthy capabilities in certain areas.

2 Market Segment

This Market Compass covers solutions that provide backup and restoration of IT service data into the cloud in the context of the hybrid IT service delivery environment that is now commonly found in medium to large organizations. These solutions provide the capability to backup IT service data together with all the necessary meta data required to make it possible to restore an exact copy of the data together with its structure and permissions to achieve given Recovery Time Objective (RTO) objectives.

2.1 Market Description

Ensuring the continuity of IT services is an essential part of the security triad of confidentiality, integrity, and availability. This requires, amongst other things, ensuring that data related to these services is backed up in a way that allows them to be restored following various unwanted events such as physical and logical damage to the storage devices or to the IT installation. To support this, organizations typically use backup solutions to take copies of this data which can then be stored safely and used, when necessary, to restore the service. These solutions provide the capability to backup IT service data together with all the necessary meta data required to make it possible to restore an exact copy of the data together with its structure and permissions to achieve given RPO/RTO objectives.

Most organizations now have a hybrid IT environment where services are delivered in multiple ways, with some remaining on premises while others are delivered as cloud services. There is a temptation to believe that the use of a cloud service removes the need for the customer to take data backups. This is only true where the SLA (Service Level Agreement) meets the customer's RPO/RTO requirements, and this is not always the case. In addition, this hybrid IT delivery model increases the management burden where multiple data protection solutions are required. This makes it important to have a common solution that covers all the different use cases.

The cloud also provides an alternative location to hold the backed-up data since major cloud services are delivered from highly secured datacentres in multiple geographic locations. These can be used to store the backed-up data with a high degree of resilience and to reduce the delays and the risks involved in the physical transfer of media to secure locations. To take advantage of this, existing legacy backup solutions have evolved, and new backup solutions have emerged.

The solutions in this market segment must accommodate the range of scenarios demanded by this hybrid IT environment including:

- Cloud backup and restoration of data from on premises services.

- Cloud backup of and restoration of data from a range of common SaaS cloud services
- Cloud backup and restoration of data for cloud-based (IaaS) applications and databases.

The inclusion and exclusion criteria for vendors are as follows:

Inclusion criteria:

- Solutions that provide cloud backup and restoration of data from IT services outside of the cloud.
- Solutions that provide cloud backup and restoration of tenants' data for widely deployed SaaS such as Office Productivity Suites, CRM, and Enterprise Applications.
- Solutions that provide cloud backup and restoration for tenants' applications and data held in IaaS including the various forms of storage and databases supported by these services.

Exclusion criteria:

- Vendors providing only managed services for backup and DR.
- Vendors providing only hardware or infrastructure for backup and DR.
- Solutions that do not support cloud services.

2.2 Major Use Cases

The main applications of these solutions are:

- **On premises protection** - the protection of data held in on premises services.
- **IaaS protection** - the protection of tenant data held in IaaS cloud services.
- **SaaS protection** - the protection of tenant data held in SaaS cloud services.
- **Disaster recovery** - the need to restore protected service data following various kinds of incident that has led to a loss of the service. This includes ransomware attacks as well as system failures and natural disasters.

2.3 Market Direction

Where IT services are delivered exclusively on-premises, these solutions can be used to make copies of the data storage media (typically tape and disk) which can then be stored in a separate location where there are additional safeguards against fire and theft. The physical transfer of these media adds delays and additional risks. There is a mature market with many existing backup and disaster recovery solutions that support this model. However, the way in which IT services are delivered is changing with the move to a hybrid model. This is leading to emerging market segments covering the protection of data in SaaS, IaaS as well as the use of cloud services to secure the backed-up data.

In our view the market for protection of SaaS and IaaS will increase significantly. In addition, CSPs are moving into this market, offering protection as a SaaS based solution - this is likely to grow.

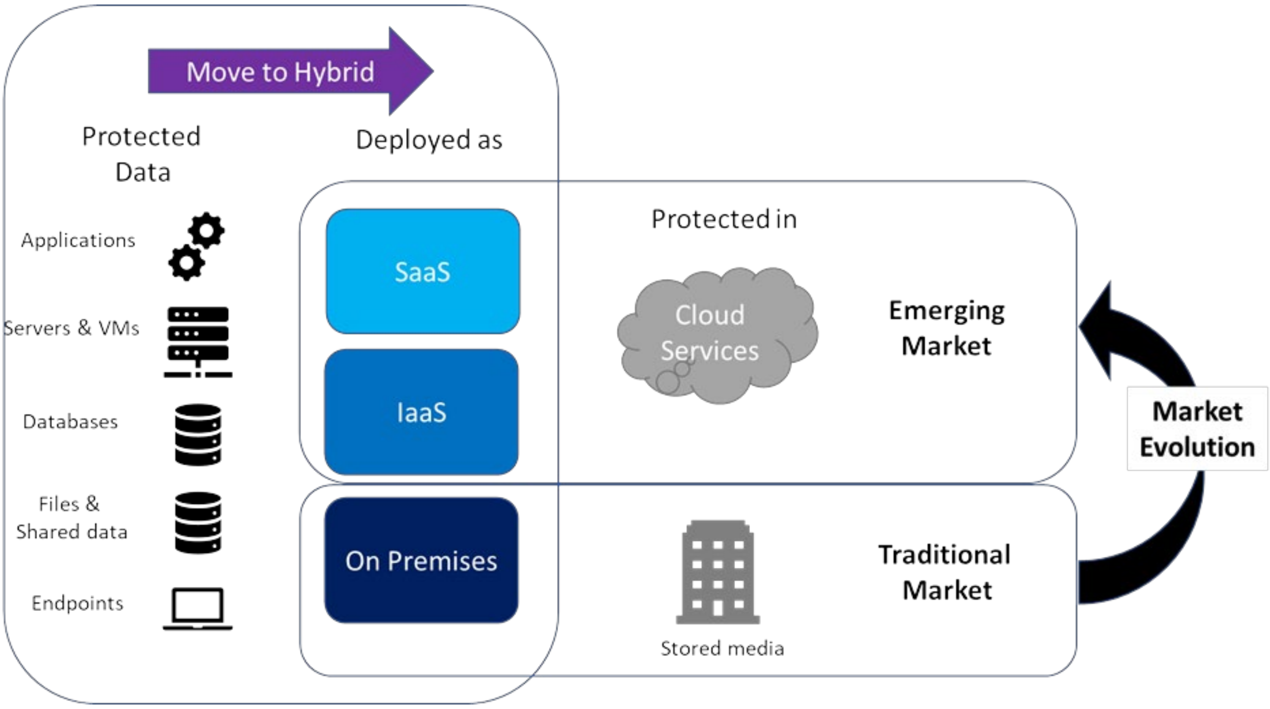


Figure 1: Market Trends

With the advent of the cloud, most organizations are now using IT services that are delivered in multiple ways. In today's hybrid and multi-cloud IT, some services remain on premises while others are delivered as cloud services. This hybrid delivery model increases the management burden especially when multiple data protection solutions are required. This makes it more important to have a common solution that covers all the different use cases.

The cloud also provides an alternative location for backed-up data since major cloud service providers usually have several highly secured datacentres in multiple geographic locations. This provides the possibility to store the backed-up data with a high degree of resilience and potentially reduces delays and the risks involved in physical transfers. This has led to the emergence of new backup solutions and the adaptation of existing solutions that backup IT service data to the cloud.

These solutions need to accommodate a range of scenarios. These include:

- Cloud backup and restoration of data from on premises services.
- Cloud backup and restoration of data from a range of SaaS cloud services. Note that there are various complexities around this that depend upon the kind of service. For example, the form of data held in shared file systems (such as Microsoft Office 365) is quite different to the form of data held in a CRM system (such as Salesforce.com).
- Cloud backup and restoration of data for cloud-based applications (IaaS) and databases.

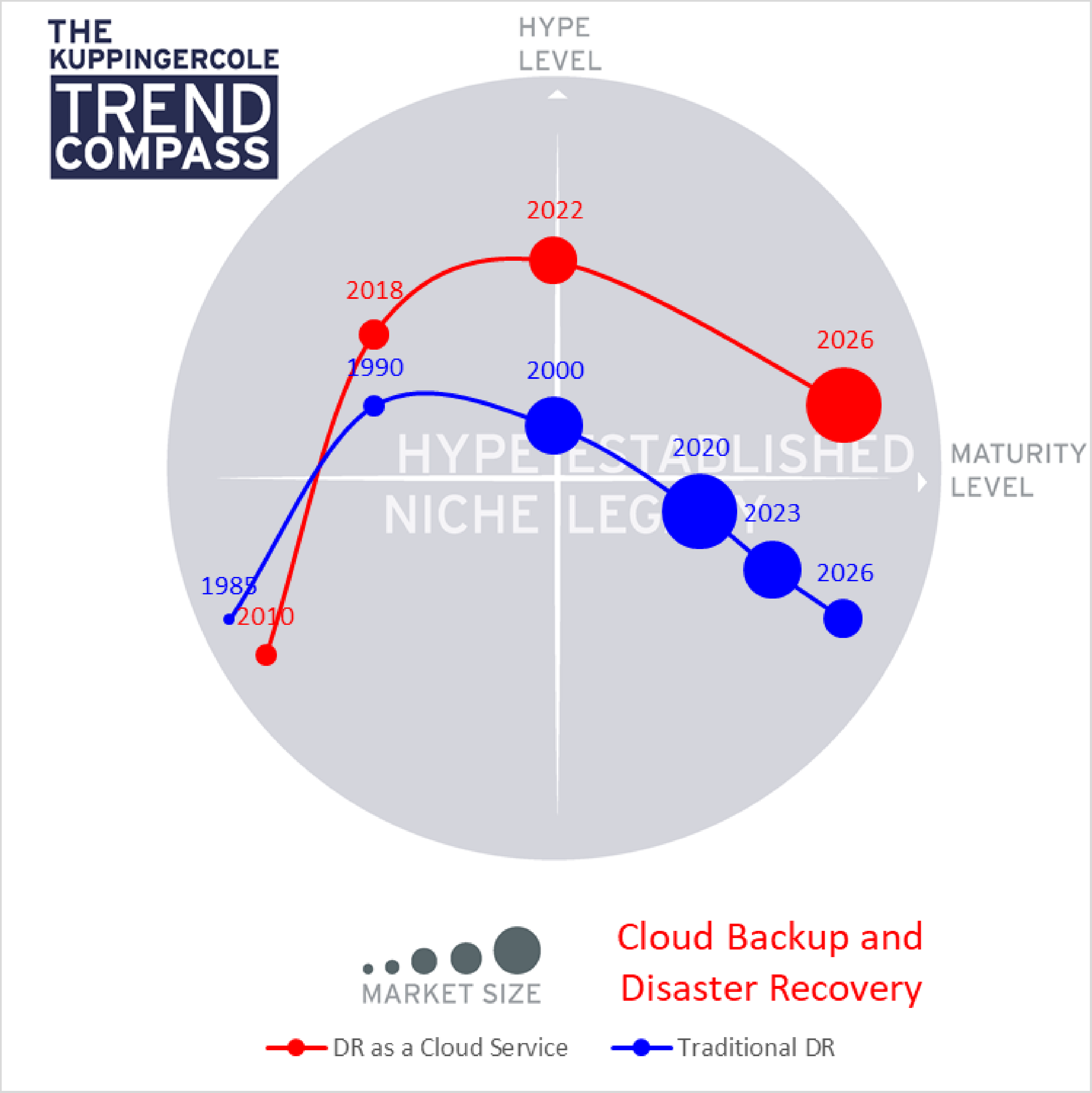


Figure 2: Disaster Recovery Market Trend from traditional tools to cloud based services

Figure 2 illustrates our view of how the market will evolve from traditional solutions (shown in blue) based on on-premises tools and managed services towards cloud-based solutions (shown in red). Currently there is large established market for traditional DR tools, but this market will decline as customers move towards cloud-based solutions. At the same time the cloud-based solutions will mature, and the market size will grow as customers migrate and digital transformation increases the need for resilience.

3 Capabilities

The Market Compass is designed to profile and compare vendors across numerous capabilities. This section details the capabilities that one should expect to see in this market segment and breaks them down according to relevance per use case.

3.1 All Capabilities

The capabilities that should be provided by Cloud Backup and Disaster Recovery are shown in the table below.

Capability	Description
Basic Capabilities	The range of capabilities the solution provides: data backup, data replication, data recovery, system restoration, continuous data protection.
	The range of storage systems and data types protected by the solution.
	The range of cloud services that the user can use to hold their protected data.
	The performance of the backup and restore processes enable realistic RTO targets.
	Durability of the backed-up data - how it is protected against deterioration.
	Deduplication - what support is provided to manage multiple copies of the protected data?
	The control provided over the frequency and content of data backed up.
Extended Capabilities	Support for near zero RTO.
	Support for continuous replication.
	Support for the migration of data and applications between different environments: on-premises to cloud, between cloud and cloud to on-premises.
	Support for data restoration for test and QA purposes
	Capabilities for data archive / long term retention.
Data Security Capabilities	Capabilities to protect the data in transit against theft, unauthorized access, and corruption.
	Capabilities to protect the backed-up data against unauthorised access, changes, and corruption.
	Capabilities to protect against malware, ransomware, and other forms of cyber-attack.

Capability	Description
	Control over administrative access for example MFA authentication.
	Support for role-based access control to enable the secure delegation and control of administration.
Compliance Capabilities	User controls over the geographic jurisdiction in which the protected data is held.
	User control over encryption and encryption keys.
	Capabilities to identify and classify sensitive data within the protected data.
	Capabilities provided to add extra protection for sensitive data.
	Audit capabilities provided by the solution.
	Independent certifications for compliance with laws and regulations across the world.
Disaster Recovery Capabilities	Capabilities for service restoration - for example: run books, workflows, and process automation.
	Full stack restoration capabilities - (i.e., the co-ordinated restoration of multiple service components)
	DRaaS (Disaster Recovery as a Service) capabilities provided
	- Fully managed service.
	- Assisted recovery providing infrastructure and help.
	- Self-service recovery.
	The guaranteed SLAs for RPO/RTO?
	Capabilities provided to support testing of the recovery processes.
SaaS Protection Capabilities	Provides a single point of control for managing the range of protected SaaS.
	Range of SaaS services covered out-of-the-box. Should include major services such as Microsoft Office 365, Google Workspace, Salesforce.
	The types of data protected out of the box for the SaaS services covered by the solution.
	Options provided for where the copies of the protected data are held.
IaaS Protection Capabilities	Provides a single point of control for managing the range of protected IaaS.
	Range of IaaS services covered out of the box. Should include major services such as AWS, GCP. IBM Cloud, Azure.
	Range of cloud DBMS are covered out of the box: For example: MS SQL, MySQL, Oracle, SAP HANA.
	Range of the types of storage found in the IaaS services e.g., files, file systems, object storage, etc.
	Support for replication of services to other regions for added DR readiness.
On Premises Protection Capabilities	Range of on premises storage and data types protected out of the box. Volumes, Databases, File Systems, File shares, OS Images, Hypervisor images, email servers and other applications.
	Range of on premises DBMS protected out of the box. MS SQL, MySQL, Oracle, SAP HANA, others?
	Range of backup media types supported.

Capability	Description
	Range of environments and applications with automated discovery and snapshots capabilities.

Table 1: All capabilities

3.2 Capabilities Recommended per use case

The Cloud Backup and Disaster Recovery market meets several distinct use cases, as described in section 2.2. Below, the capabilities are displayed according to their relevance for each use case.

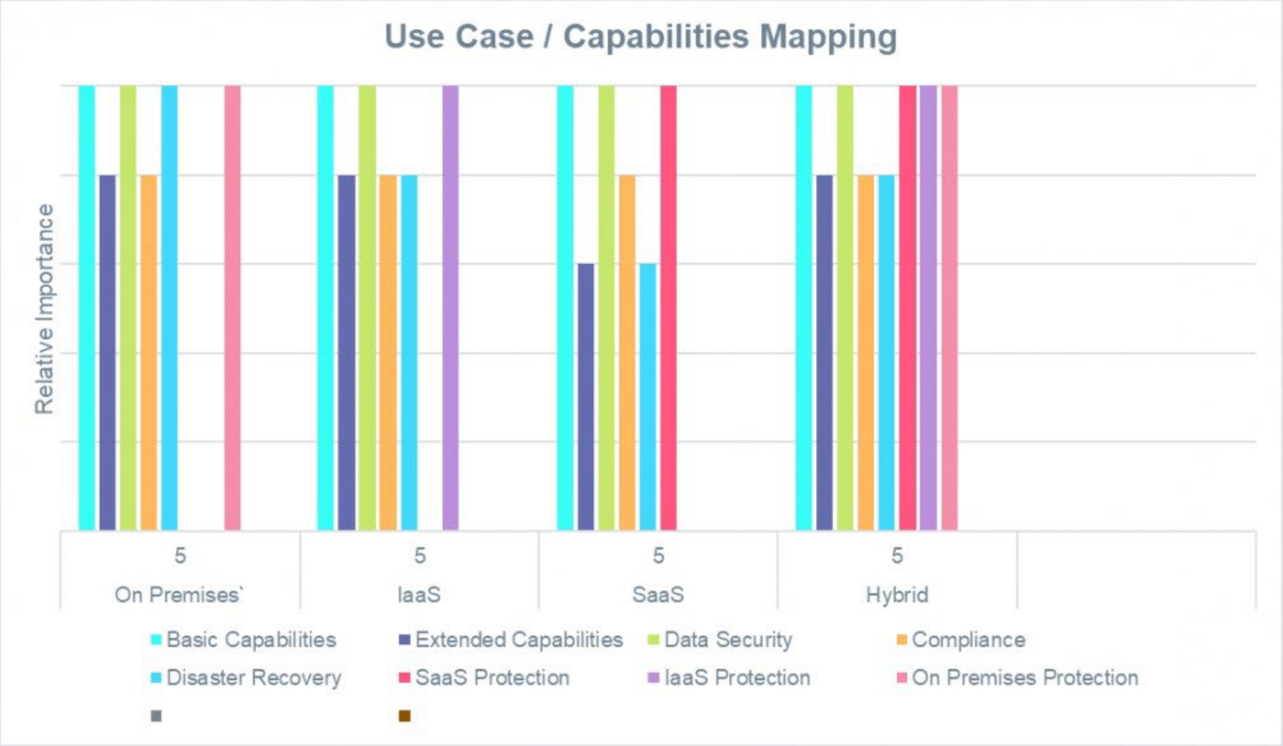


Figure 3: Relative importance of capabilities for each use case

3.2.1 On Premises Use Case

In this use case the objective is to be able to protect data and services that are being hosted on premises.

Essential capabilities for the on-premises protection use case are:

- Basic Capabilities
- Data Security
- Disaster recovery capabilities
- On-premises protection capabilities.

Recommended Capabilities for the on-premises protection use case are:

- Extended capabilities
- Compliance capabilities appropriate for the organization.

The other capabilities not relevant to this use case.

3.2.2 IaaS User Case

In this use case the objective is to be able to protect data and services that are being hosted in IaaS.

Essential capabilities for the IaaS protection use case are:

- Basic Capabilities
- Data Security
- Disaster recovery capabilities
- IaaS protection capabilities.

Recommended Capabilities for the IaaS protection use case are:

- Extended capabilities
- Compliance capabilities appropriate for the organization.

The other capabilities not relevant to this use case.

3.2.3 SaaS User Case

In this use case the objective is to be able to protect data that are being hosted in SaaS.

Essential capabilities for the SaaS protection use case are:

- Basic Capabilities
- Data Security
- Disaster recovery capabilities
- SaaS protection capabilities.

Recommended Capabilities for the SaaS protection use case are:

- Extended capabilities
- Compliance capabilities appropriate for the organization.

The other capabilities not relevant to this use case.

3.2.4 Hybrid User Case

In this use case the objective is to be able to protect data that are being delivered through a combination of on-premises, IaaS, and SaaS.

Essential capabilities for the hybrid protection use case are:

- Basic Capabilities
- Data Security
- Disaster recovery capabilities
- On premises Protection
- IaaS Protection Capabilities
- SaaS protection capabilities.

Recommended Capabilities for the SaaS protection use case are:

- Extended capabilities
- Compliance capabilities appropriate for the organization.

4 Ratings at a Glance

This chapter provides a comparative overview of the participating vendors for five categories: security, deployment, interoperability, usability, and market standing. It also highlights the outstanding performers in each of the capabilities that were assessed.

4.1 General Product Ratings

Based on our evaluation, a comparative overview of the ratings of the general standing of all the products covered in this document is shown in table 1.

Product	Security	Interoperability	Usability	Deployment	Market Standing
Acronis Cyber Protect 15	●	○	●	●	○
Arcserve Unified Data Protection 8.1	●	●	●	●	○
AWS CloudEndure	●	○	○	●	●
Cobalt Iron Compass	●	●	●	●	🟡
Cohesity DataProtect and SiteContinuity	●	●	●	●	🟡
Commvault Intelligent Data Management Platform	●	●	●	●	●
Datto Unified Continuity	●	○	○	●	○
Dell Technologies – PowerProtect Portfolio	●	●	●	●	●
Druva Data Resiliency Cloud	●	○	●	●	🟡
Google Actifio Backup and Recovery	●	○	○	●	●
IBM Spectrum Protect Plus	●	○	●	●	●
iland Secure DRaaS?	●	🟡	○	●	○
Micro Focus Data Protector	●	○	○	●	●
Microsoft Azure Backup and Azure Site Recovery	●	🟡	●	●	●
Unitrends Backup and DRaaS Software	●	●	●	●	🟡
Veeam Backup & Replication V11	●	○	○	●	○
Veritas NetBackup 9.1	●	●	●	●	●
Zerto Platform	●	○	○	●	○

Legend 🔴 critical 🟠 weak 🟡 neutral ○ positive ● strong positive

5.1 Arcserve

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 NetBackup in 1988. It was 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.

This report covers Arcserve Unified Data Protection (UDP) 8.1. Arcserve UDP 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.

Arcserve UDP comes as software or a converged appliance (software plus hardware for storing the backup data: 9000 series, X series and N Series). The N Series Appliances are powered by Nutanix and secured by Sophos. This provides the scale-out capabilities of Nutanix and the ransomware defence of Sophos Intercept X Advanced cybersecurity. It supports an incremental forever backup approach with each recovery point being independent to ensure rapid backups without recovery points being dependant on each other.

It enables protection of a broad range of platforms, including Windows, Linux, Amazon EC2, Microsoft Azure, Office 365 (Exchange Online, SharePoint Online and OneDrive for Business), Microsoft Exchange, MS SQL, file servers, Microsoft IIS, Microsoft Active Directory, Oracle Database, PostgreSQL, VMware vSphere (agentless), Microsoft Hyper-V (agentless) and Nutanix AHV (agentless). Backup of data to the cloud requires an on-premises server to manage replication and deduplication.

UDP exploits cloud-native capabilities to integrate on- and off-site backup and rapid 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 Arcserve UDP solution 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. Integration with the OneXafe immutable object-based scale-out NAS storage appliance (coming from StorageCraft) provides an on premises immutable storage backup target for UDP.

Arcserve UDP Cloud Direct DRaaS provides failover capabilities for on-premises servers by transferring images to the Arcserve Cloud Direct infrastructure. In the event of a disaster, these backup images are used to run virtual instances of the servers in the Arcserve Cloud Direct infrastructure. Users are able to access these via secure virtual private network (VPN) connectivity. Arcserve Cloud Direct is provided from datacentres in Santa Clara, CA, Secaucus, NJ, Manchester (UK), and Japan.

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 InstantVM enables these to be spun up as virtual machines on-demand in the backup environment.

UDP also provides protection for Microsoft Office 365 OneDrive for Business Microsoft Office 365 Exchange Online Microsoft Office 365 SharePoint Online Microsoft Office 365 Teams data.

Arcserve UDP 8.1 is a mature product with comprehensive functionality and a strong user base. It enables centralized management and control of data protection across physical, virtual and cloud environments.

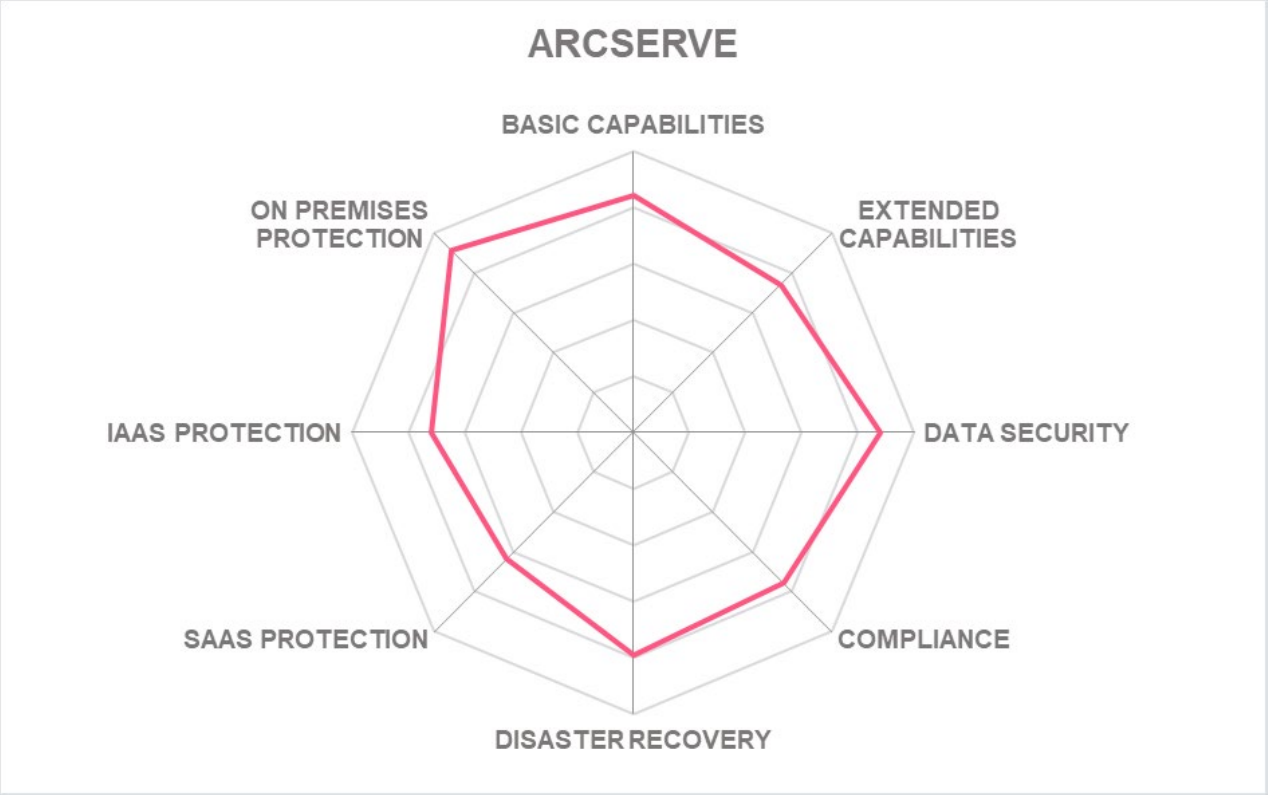
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Market Standing	● ● ● ● ○

Strengths

- Mature product with strong user base.
- Comprehensive functionality covers multiple use cases.
- Agentless VM Ware and Hyper-V and Nutanix protection.
- Integrated deduplication.
- Wide choice of cloud for backup storage and disaster recovery.
- Coverage of Microsoft Office 365.
- Exploits AWS S3 Object lock to provide backup immutability.
- Integration with Sophos X provides protection against cyber threats.
- Arcserve UDP Cloud Direct provides direct-to-cloud backup and disaster recovery as a service.
- Support for disaster recovery through VM images in the cloud.
- Arcserve Assured Recovery™ testing enables validation of RPO/RTO.

Challenges

- Integration of the business and technology with StorageCraft.
- Protection for SaaS services is limited to Microsoft Office 365.
- 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 tier long term retention capabilities.


ARCSERVE
BASIC CAPABILITIES
EXTENDED CAPABILITIES
DATA SECURITY
COMPLIANCE
DISASTER RECOVERY
SAAS PROTECTION
IAAS PROTECTION
ON PREMISES PROTECTION

6 Related Research

Architecture Blueprint: Hybrid Cloud Security - 72552
Advisory Note: Maturity Level Matrix for Cyber Security - 72555
Advisory Note: GRC Reference Architecture - 72582
Advisory Note: Protect Your Cloud Against Hacks and Industrial Espionage - 72570
Advisory Note: Security Organization Governance and the Cloud - 72564
Advisory Note: Cloud Services and Security - 72561
Advisory Note: How to Assure Cloud Services - 72563
Advisory Note: Firewalls Are Dead - How to Build a Resilient, Defendable Network - 72163
Architecture Blueprint: Access Governance and Privilege Management - 79045
Architecture Blueprint: Identity and Access Management - 72550

Methodology

About KuppingerCole's Market Compass

KuppingerCole Market Compass is a tool which provides an overview of a particular IT market segment and identifies the strengths of products within that market segment. It assists you in identifying the vendors and products/services in that market which you should consider when making product decisions.

While the information provided by this report can help to make decisions it is important to note that it is not sufficient to make choices based **only** on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e., a complete assessment.

Product Rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Deployment
- Interoperability
- Usability
- Market Standing

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

Market Standing is a measure of financial strength and market position. This is based on publicly available information, and takes the amount of funding received, the profitability, and the private or public status of the vendor into consideration.

We focus on security, deployment, interoperability, usability, and market standing for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Rating scale for products

For vendors and product feature areas, we use a separate rating with five different levels. These levels are:

- **Strong positive**

Outstanding support for the subject area, e.g. product functionality, or security etc.)

- **Positive**
  Strong support for a feature area but with some minor gaps or shortcomings. Using Security as an example, this could indicate some gaps in fine-grained access controls of administrative entitlements.
- **Neutral**
  Acceptable support for feature areas but with several of our requirements for these areas not being met. Using functionality as an example, this could indicate that some of the major feature areas we are looking for aren’t met, while others are well served.
- **Weak**
  Below-average capabilities in the area considered.
- **Critical**
  Major weaknesses in various areas.

Copyright

All conclusions, recommendations and predictions in this document represent KuppingerCole´s initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice.

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company 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.