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
Content

1 Management Summary ........................................... 4

2 Market Segment .................................................. 5
   2.1 Market Description ......................................... 5
   2.2 Market Direction ........................................... 6
   2.3 Capabilities .................................................. 9
      2.3.1 Basic Functionality ...................................... 9
      2.3.2 SaaS Protection .......................................... 12
      2.3.3 IaaS Protection .......................................... 13
      2.3.4 On Premises Protection .................................. 15
      2.3.5 Disaster Recovery ........................................ 18

3 Vendors and Products .......................................... 20
   3.1 Vendors covered .............................................. 20
   3.2 Featured Vendors ............................................. 21
      3.2.1 Featured for innovation .................................. 21
      3.2.2 Featured for SaaS protection ............................... 23
      3.2.3 Featured for Comprehensive Capabilities ................. 23
   3.3 Vendors to watch .............................................. 25

4 Ratings at a glance ............................................. 27

5 Product/Service Evaluation ................................... 30
   5.1 Acronis ......................................................... 31
   5.2 Actifio .......................................................... 34
   5.3 Arcserve ......................................................... 37
   5.4 Amazon Web Services ....................................... 40
   5.5 Cobalt Iron ...................................................... 43
   5.6 Commvault ....................................................... 46
   5.7 Dell EMC ......................................................... 49
   5.8 IBM ............................................................. 52
   5.9 iland ............................................................ 55
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 the 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. 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 the required recovery objectives.

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. Some cloud service users believe that the service itself provides all the continuity that they need. This may or may not be true, but it is up to the cloud customer to check that the service SLA meets their needs. However, there is now an emerging market for solutions that provide back-up protection for cloud service data.

Most of the existing vendors are adapting their solutions to this new model but most still have some way to go, especially in the area of SaaS. 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, and especially for Microsoft Office 365, several new vendors now offer solutions for customers to back-up the data held in the SaaS services they use.

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 than 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.
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 held in these services is backed up in a way that allows them to continue following various unwanted events such as physical and logical damage to the storage devices or the IT installation. To cater for this organizations typically use backup solutions to take copies of the data which can then be stored safely and used if it becomes necessary to restore the service. These solutions must also provide the capabilities to restore the selected backup data, together with all its structure and meta data in a timely manner to achieve a given RTO.

All organizations need to consider the risks related to the availability of their business data and take appropriate measures to mitigate these risks. In most cases this will involve investing in either or both backup products and disaster recovery services.

- The backup products take regular copies or snapshots of critical data in a form that enables that data to be quickly restored.
- To protect the backed-up data against loss or damage this data must be stored separately and storing backup data in cloud services is now a common solution for this.
- Data held in cloud services also needs to be backed up. This is often assumed to be the responsibility of the cloud service provider. Organizations need to check that the SLA for this meets their business needs. Especially for SaaS.
- Disaster recovery services provide managed services to assist organizations with the processes involved in the above.

This report describes the basic capabilities that all solutions should support. It then looks in more detail at the capabilities required for the different market segments which are:
• **On premises protection** – this is where the existing solutions are mostly to be found
• **IaaS protection** – solutions that cover the protection of data held in IaaS cloud services
• **SaaS protection** – solutions that cover the protection of data held in SaaS.
• **Disaster recovery** – all solutions should provide this capability, but many vendors and third parties offer services to support this. This report covers the capabilities of the solutions themselves but does not cover the large market in DR services.

### 2.2 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 service – this is likely to grow.
With the advent of the cloud most organizations are now using IT services that are delivered in multiple ways. In today’s hybrid multi-cloud IT, some services remain 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 RTO requirements, and this is not always the case. In addition, this hybrid delivery model increases the management burden where 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 of 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 1: 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 customer migrate and digital transformation increases the need for resilience.
2.3 Capabilities

The precise functionality provided by the solutions depends upon the scenario and the source of the IT service data described above. Not all solution might cover all scenarios. This section describes the capabilities that are required.

2.3.1 Basic Functionality

The basic functionality that should be provided by all solutions solution includes:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
<th>Relevance</th>
<th>On-premises Protection</th>
<th>SaaS Protection</th>
<th>IaaS Protection</th>
<th>Disaster Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Support</td>
<td>The solution should enable the backup and restoration of data to a cloud service. Ideally the organization using the solution should be able to choose the cloud service used or at least the region.</td>
<td>Essential</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Performance</td>
<td>The process for backing up and restoring the data should be adequately performant and efficient allowing service to continue operation during the backup process and enabling the RTO needed by the organization using the solution.</td>
<td>Essential</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Capability</td>
<td>Description</td>
<td>Relevance</td>
<td>On-premises Protection</td>
<td>SaaS Protection</td>
<td>IaaS Protection</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Data Location</strong></td>
<td>The organization using the solution should be able to control the geographic jurisdiction in which the backed-up data is held.</td>
<td>Essential</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Durability</strong></td>
<td>The backed-up data should be protected against deterioration so that it can be recovered unchanged later. The guaranteed life of the backed-up data should be defined in an SLA.</td>
<td>Desirable</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>De-duplication</strong></td>
<td>Support for managing multiple copies of the same data. This can reduce the cost of storage as well as the cost of data transfers where it is done at source. It can also remove multiple copies of sensitive data potentially reducing compliance risks.</td>
<td>Recommended</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Restorability</strong></td>
<td>The solution should ensure that the backed-up data can be restored together with its structure and meta data such as permissions automatically within the required RTO.</td>
<td>Essential</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Capability</td>
<td>Description</td>
<td>Relevance</td>
<td>On-premises Protection</td>
<td>SaaS Protection</td>
<td>IaaS Protection</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Secure transfer</strong></td>
<td>The solution should ensure that the data in transit to and from the backup location is secured against unauthorized access, leakage and eavesdropping.</td>
<td>Essential</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Data security</strong></td>
<td>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. This could be achieved through encryption where the customer controls the keys.</td>
<td>Essential</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>The backed-up data as well as the backup and restoration process should be compliant with the laws and regulations required by the organization using it.</td>
<td>Recommended</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Administrative functionality</strong></td>
<td>To control backup frequency and content must be provided. It should also include the capability to delegate administration in a granular manner.</td>
<td>Essential</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
### 2.3.2 SaaS Protection

Increasingly organizations are using 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 may be too long or there may be inadequate protection against customer errors. These solutions provide protection for data held in SaaS services and, in addition to the basic capabilities, their functionality should include:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
<th>Relevance</th>
<th>On-Premises Protection</th>
<th>SaaS Protection</th>
<th>IaaS Protection</th>
<th>Disaster Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single point of</td>
<td>They should provide a single control point and management interface for the</td>
<td>Essential</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>controls</td>
<td>range of protected SaaS services.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protected services</td>
<td>This range of services covered should include and as well as other popular services.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>Essential</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>365</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G Suite</td>
<td>Recommended</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salesforce.com</td>
<td>Recommended</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other services</td>
<td>Optional</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Capability</td>
<td>Description</td>
<td>Relevance</td>
<td>On-Premises Protection</td>
<td>SaaS Protection</td>
<td>IaaS Protection</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Protected Data</td>
<td>The data backed up will depend upon the service. It would typically include:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For Office 365: Emails, Calendar, Contacts, Tasks, Shared Mailbox, In-place archive, OneDrive, SharePoint, Groups and Team Sites</td>
<td>Essential</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For G Suite: Emails, Calendar, Tasks, Google drive, Team drive, Sites, Docs</td>
<td>Recommended</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For Salesforce.com: Accounts, Contacts, Leads, Opportunities, Activities, Notes, Cases, Custom fields on the previous.</td>
<td>Recommended</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>There should be control over what is backed up and how often as well as over restore allowing selective and partial restores depending upon the needs.</td>
<td>Essential</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Manage Multiple Services</td>
<td>Support to manage multiple services.</td>
<td>Recommended</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

2.3.3 IaaS Protection
Increasingly business critical applications are being deployed using IaaS and, while the CSP is responsible for the infrastructure, the customer is responsible for their data. These solutions should provide protection for applications and data held in IaaS clouds and in addition to the basic capabilities they should provide:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
<th>Relevance</th>
<th>On-Premises Protection</th>
<th>SaaS Protection</th>
<th>IaaS Protection</th>
<th>Disaster Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single point of controls</td>
<td>They should provide a single control point and management interface for the range of protected services.</td>
<td>Essential</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Protected Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>AWS Cloud</td>
<td>Essential</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Google Cloud Platform</td>
<td>Recommended</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>IBM Cloud</td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Essential</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Other services</td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Protected Cloud DBMS</td>
<td>Support to protect data held in DBMS in the cloud services. Typically, these should include: MySQL, Oracle, Microsoft SQL Server, PostgreSQL, Others</td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Automated discovery</td>
<td>It should feature automated discovery and backup of data and cover snapshots for a wide range of environments and applications. It should provide the ability to search and restore down to the file-level.</td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Capability</td>
<td>Description</td>
<td>Relevance</td>
<td>On-Premises Protection</td>
<td>SaaS Protection</td>
<td>IaaS Protection</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Replication</td>
<td>It should enable the replication of the service to other regions for added disaster recovery readiness.</td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Classification</td>
<td>For compliance purposes the ability to classify, identify and manage controls over Personally Identifiable Information in backups.</td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

### 2.3.4 On Premises Protection

The solution should provide the capability to protect data held in on premises IT services. It should support:
<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
<th>Relevance</th>
<th>On-Premises Protection</th>
<th>SaaS Protection</th>
<th>IaaS Protection</th>
<th>Disaster Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protected Data</strong></td>
<td>Protection for a range of types of data including: Volumes (whole disk/tape backup and restore), Databases (whole or partial database backup and restore), File Systems (whole or partial backup/restore of a file system), File shares (shared file store backup and restore), OS Image (backup/restore of OS image), Hypervisor (backup and restore of hypervisor image), Email (backup/restore of email server and associated content), Application specific data backup/restore</td>
<td>Essential</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Capability</td>
<td>Description</td>
<td>Relevance</td>
<td>On-Premises Protection</td>
<td>SaaS Protection</td>
<td>IaaS Protection</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Backup Media Emulation</td>
<td>Backup solutions often work by writing the protected data to tape, disk of tape library devices. The cloud-based solution should provide compatibility through emulation of these so that it works seamlessly across different protected environments. This is also important because it provides a route to move the backed-up data out of the cloud service should this be needed.</td>
<td>Recommended</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Choice of Cloud Service</td>
<td>Choice of Cloud Service used through connectors including: AWS, Microsoft®, Google Cloud, Oracle Cloud, IBM Cloud, Other services including region- and industry-specific ones.</td>
<td>Recommended</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated discovery</td>
<td>It should feature automated discovery and backup of data and cover snapshots for a wide range of environments and applications. It should provide the ability to search and restore down to the file-level.</td>
<td>Recommended</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recommended**

<p>| IBM Cloud                     | Recommended                                                                                                                                |                 |                       |                 |                 |                  |
| Microsoft Azure               | Essential                                                                                                                                  |                 | x                      |                 |                 | x                 |
| Other services                | Recommended                                                                                                                                | x               | x                      | x               |                 |                  |</p>
<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
<th>Relevance</th>
<th>On-Premises Protection</th>
<th>SaaS Protection</th>
<th>IaaS Protection</th>
<th>Disaster Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protected Cloud DBMS</strong></td>
<td>Support to protect data held in DBMS in the cloud services. Typically, these should include: MySQL, Oracle, Microsoft SQL Server, PostgreSQL, Others</td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td><strong>Automated discovery</strong></td>
<td>It should feature automated discovery and backup of data and cover snapshots for a wide range of environments and applications. It should provide the ability to search and restore down to the file-level.</td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td><strong>Replication</strong></td>
<td>It should enable the replication of the service to other regions for added disaster recovery readiness.</td>
<td>Recommended</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>For compliance purposes the ability to classify, identify and manage controls over Personally Identifiable Information in backups.</td>
<td>Recommended</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

### 2.3.5 Disaster Recovery

The solution should provide the capability for disaster recovery. It should support:
<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
<th>Relevance</th>
<th>On-Premises Protection</th>
<th>SaaS Protection</th>
<th>IaaS Protection</th>
<th>Disaster Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRaaS</td>
<td>Disaster Recovery as a Service (DRaaS) based on the use of cloud services.</td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Range of DRaaS</td>
<td>The range of DRaaS services covered should include:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A fully managed service covering all aspects</td>
<td></td>
<td>If needed</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Assisted recovery is where the offering provides the recovery infrastructure and manages data replication</td>
<td></td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Self-service recovery the solution provides the tools needed to accomplish the various tasks</td>
<td></td>
<td>Essential</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Defined Recovery SLA</td>
<td>DRaaS should provide defined SLAs for:</td>
<td>Essential</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>RTO (Recovery Time Objectives)</td>
<td></td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>RPO (Recovery Point Objectives)</td>
<td></td>
<td>Recommended</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Security/Compliance Certifications</td>
<td>DRaaS service should be independently certified / attested to: ISO/IEC 27001, PCI/DSS, SAE 16 SOC 2</td>
<td>If needed</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
3 Vendors and Products

The vendors in the market covered by this report are those with products that enable backup and disaster recovery for data deployed on premises, in IaaS and SaaS including the ability to use cloud services for storing the protected data and for disaster recovery.

3.1 Vendors covered

These vendors covered in this report are:

- **Acronis** was founded in Singapore in 2003 and incorporated in Switzerland in 2008. It provides a range of data protection and disaster recovery solutions including Acronis Cyber Backup.

- **Actifio** is a privately held information technology firm headquartered in Waltham, Massachusetts. Actifio provides an incremental backup solution.

- **Arcserve** is a global company with headquarters in Eden Prairie, Minnesota in the USA. This report covers Arcserve Unified Data Protection (UDP) 7.0.

- **AWS CloudEndure** offers Disaster Recovery and Migration Software-as-a-Service (SaaS) solutions into Amazon Web Services (AWS).

- **Cobalt Iron** is a private company with headquarters in Lawrence, Kansas in the USA. It offers Cobalt Iron Compass which is a SaaS solution for enterprise backup.

- **Commvault** was formed in 1988 as a development group within Bell Labs, and later designated as a strategic business unit of AT&T Network Systems. In 1996, it was incorporated as an independent company. It provides a range of products for backup and disaster recovery.

- **Dell Technologies** is a multinational corporation with headquarters in Round Rock, Texas. This report covers the Dell EMC Data Protection Suite.

- **IBM Spectrum Protect™** provides scalable data protection for physical file servers, applications, and virtual environments. Additionally, IBM offers a fully managed DRaaS.

- **Micro Focus** is a global infrastructure software business. In 2017 Micro Focus closed the deal to acquire HPE software business and, as part of this acquisition, obtained HPE Data Protector backup and disaster recovery solution which is now sold as Micro Focus Data Protector.

- **Microsoft** is a global provider of cloud, infrastructure and software services. Microsoft Azure is their IaaS offering and in June 2018, Microsoft announced the general availability of Azure Site Recovery.
to replicate and protect IaaS based applications running on Azure.

- **Rubrik** is a multi-cloud data control company based in Palo Alto, California, United States founded in December 2013. It provides products for backup and recovery across hybrid cloud environments.

- **Unitrends Inc.** is a Kaseya company, a US-based company specializing in backup and business continuity.

- **Veeam Software** was founded in 2006 and was acquired in February 2020 by Insight Partners. This report focuses on Veeam Availability Suite 10.

- **Veritas** is a global business with headquarters in the USA and an annual revenue of over $2 Billion. This report focuses on Veritas NetBackup™ 8.2.

### 3.2 Featured Vendors

All the vendors that we reviewed in this market segment offer strong basic functionality and protection for on premises workloads as well as security. The differences can be seen in the other aspects notably the lack of wide coverage for the protection of SaaS. This section highlights several vendors that illustrate different aspects of the market.

#### 3.2.1 Featured for innovation
Acronis Notary

protects backed up data against change and tampering using Acronis Notary. Acronis Notary is based on Blockchain technology and used for timestamping and fingerprinting any data objects and streams. After a backup, Acronis calculates and sends file hash codes to the Acronis Notary service. A hash code is a unique fixed size number that is produced by a hash function. This code mathematically defines an arbitrary set of data, for example, a backup file. Any change of the backup file leads to a change of its hash code. When Acronis Notary receives hash codes of the protected files, it calculates a new single hash code and sends it to the Ethereum Blockchain-based database. This is useful because during recovery, in the solution interface, the notarized files will be marked with a special icon so an administrator or a corporate employee can verify the file authenticity.

AWS CloudEndure

AWS is a well-known hyperscale cloud service provider offering strong long-term cloud storage capabilities with block, file and virtual tape interfaces which have been exploited by backup and disaster recovery products. It also offers workload and replication capabilities which can be used by workloads running within AWS.

In January 2019, AWS acquired CloudEndure and Israeli company that was previously an AWS partner. CloudEndure offers Disaster Recovery and Migration Software-as-a-Service (SaaS) solutions into Amazon Web Services (AWS). Both solutions are powered by CloudEndure’s innovative workload mobility technology, which continuously replicates applications from physical, virtual, or cloud-based infrastructure to
a low-cost “staging area” that is automatically provisioned in the customer’s chosen AWS Region. CloudEndure works at the raw device level, copying blocks from the disk as they are written. This means that any application version, even proprietary house developed apps, can be protected and replicated/migrated into AWS. During failover, cutover, or testing, an up-to-date copy of applications can be spun up on demand and rapidly be fully functional. CloudEndure Migration supports migration to AWS from on-premises environments, including physical and virtual infrastructure, all private clouds, and public clouds including Microsoft Azure, Google Cloud Platform (GCP), OpenStack, Oracle Cloud, CloudStack, and IBM Cloud as well as from another AWS account or AWS Region.

3.2.2 Featured for SaaS protection

![Figure 4: Featured for SaaS Protection](image)

**Unitrends**

Unitrends is a long-time vendor in this market with a focus on SME customers. In 2018, Unitrends was acquired by Kaseya, with headquarters in Miami, Florida in the USA. Unitrends offers a variety of backup and disaster recovery solutions that include coverage for on-premises, cloud apps and SaaS with a range of storage options including public cloud.

Through this acquisition Unitrends now offers Spanning Backup for Office 365. This provides protection for with automated backup including unlimited storage and point-in-time, granular restore of mail, calendar, OneDrive, and SharePoint. In our trials this was the most comprehensive and easiest to use solution for protection of Office 365.
3.2.3 Featured for Comprehensive Capabilities

Commvault Complete™ Backup & Recovery

This is one of several products that provide comprehensive backup and disaster recovery including:
Commvault HyperScale™ for hyperscale scale-out, Commvault Orchestrate™ for end-to-end data syncing
for faster disaster recovery, and workload migration, and Commvault Activate™ provides insight into data for
data governance and compliance.

As well as providing standard backup and recovery functionality to store protected data on tape/disk media,
including deduplication and encryption capabilities it can store protected data with common cloud storage
providers (Amazon, Microsoft, Google and more). It fully supports all file systems, applications, databases
and virtualization platforms. It also provides protection for endpoints as well as Google Apps and Database,
Microsoft Office 365 and Salesforce.com. Partners provide managed services for DR.

Veritas NetBackup 8.2

This is a leading product with comprehensive functionality and a strong user base. It provides backup and
recovery of business data across hybrid, physical, virtual and multi-cloud environments.

It scales to support large workloads and delivers capabilities for virtualized and cloud-based deployments. It
supports a wide range of environments and integrates with every layer of the infrastructure stack.
NetBackup integrates with hypervisors including VMware vSphere®, Microsoft® Hyper-V, Nutanix AHV, Red Hat Virtualization and OpenStack. It integrates with relational database and application platforms, including IBM DB2®, Microsoft® Exchange Server, Microsoft SQL Server®, MySQL™, Oracle®, SAP® and others. It supports data protection for Microsoft Office 365, Google G-Suite and Salesforce SaaS services. It supports third-party cloud storage providers such as AWS, Microsoft® Azure and Google that can be incorporated into NetBackup policies.

3.3 Vendors to watch

For some time, cloud services have been used to store protected data and for disaster recovery by backup and DR products. The cloud vendors are now entering this market with their own products. However, cloud vendors that only provide the capability to protect the data and services held in their own cloud are not included in this report.

One major area where current products are lacking is protecting data held in SaaS some vendors are now introducing this capability for a limited range of services. The rationale behind this is that while the SaaS vendor protects against loss of data because of infrastructure failures they do not cover loss due to mistakes such as accidental deletion by the customer.

There is also a market for Disaster Recovery as a managed service. Many of the vendors in this report also offer this either directly or through partners. Vendors that mainly offer managed disaster recovery services are not included in the report – these include:

**C&W Business** with headquarters in Coral Gables FL has data centres around the North America and the Caribbean. It offers DRaaS based on these.

Why worth watching: C&W has a series of integrated solutions to automate and orchestrate a very wide range of platforms.

**Expedient** with headquarters in Pittsburgh OH, provides a range of managed and cloud services including their Push Button DR which offers network failover between disparate locations.

Why worth watching: Expedient’s Push Button DR offers rapid, total network failover between disparate locations at the push of a button, without IP or DNS changes.

**Flexential** with headquarters in Charlotte, NC provides the Flexential Recovery Cloud (DRaaS).

Why worth watching: Flexential's Recovery Cloud guarantees the customer’s IT environment is always on and compliant with regulatory requirements, and the “as-a-service” model means no upfront capital investments.

**InterVision Systems LLC**, which was founded in 1993, with headquarters in St. Louis MO and Santa Clara CA, provides a range of managed services including DRaaS.
Why worth watching: Covers workload in the AWS cloud, on-premise or in a hybrid configuration, the ability and provides the failover and failback operations critical to keeping the business running.

SunGard Availability Services provides IT production and recovery services with annual revenues of approximately $1.4 billion and offices in 9 countries.

Why worth watching: a long time provider of disaster recovery, with services to support both physical and virtual recovery scenarios backed by SLAs.

Recovery Point is a DRaaS provider with headquarters in Gaithersburg, MD 20878. Its service covers mainframes as well as x86 architecture servers.

Why worth watching: Recovery Point has a long experience supporting complex, heterogeneous environments, as well, including: IBM Z Series, IBM I, AIX, HPUX and Oracle as well as x86 environments.

TierPoint with headquarters in St. Louis, MO provides information technology and services including DRaaS.

Why worth watching: TierPoint offer a variety of configurations with failover options to a TierPoint private or multitenant cloud. The customer can select from fully managed or self-service recovery and testing solutions.
Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in table 1.
<table>
<thead>
<tr>
<th>Product</th>
<th>Security</th>
<th>Interoperability</th>
<th>Usability</th>
<th>Deployment</th>
<th>Basic Protection</th>
<th>On-Premises</th>
<th>IaaS</th>
<th>SaaS</th>
<th>Disaster Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acronis Cyber Backup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actifio SKY/CDS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arcserve Unified Data Protection 7.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS CloudEndure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cobalt Iron Compass</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commvault Complete™ Backup &amp; Recovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dell EMC Data Protection Suite</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Spectrum Protect Plus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iland DRaaS?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Micro Focus Data Protector</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Azure Site Recovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rubrik Cloud Data Management V5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unitrends Backup and DRaaS Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Veeam Availability Suite 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Veritas NetBackup™ 8.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend: ![critical](critical), ![weak](weak), ![neutral](neutral), ![positive](positive), ![strong positive](strong positive)
5 Product/Service Evaluation

Spider graphs

In addition to the ratings for our standard categories we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the Market Compass. For this Market Compass, we look at the following areas:

- **Basic Protection**
  How well the product or service provides basic protection for data based on the capabilities described in section 2.3.1.

- **On-premises protection**
  How well the product or service provides protection for data held in on-premises services based on the capabilities described in sections 2.3.1 and 2.3.4.

- **IaaS protection**
  How well the product or service provides protection for data held in IaaS services based on the capabilities described in sections 2.3.1 and 2.3.3.

- **SaaS protections**
  How well the product or service provides protection for data held in SaaS services based on the capabilities described in sections 2.3.1 and 2.3.2.

- **Disaster recovery**
  How well the product or service provides the ability for the customer to recover their data and restore the service following an incident based on the capabilities described in sections 2.3.

These spider graphs provide comparative information by showing the areas where the products are stronger or weaker. Some products may have gaps in some areas, while being strong in others. These might be a good fit if only the specific features are required. Other services deliver strong capabilities across all areas, thus being a better fit for strategic choice of product.
5.1 Acronis

Acronis was founded in Singapore in 2003 and incorporated in Switzerland in 2008. Acronis now has more than 1,500 employees in 18 countries. It provides a range of data protection and disaster recovery solutions including Acronis Cyber Backup and Acronis Disaster Recovery Service (formerly nScaled DRaaS) using its cloud services.

Acronis Cyber Backup provides cyber protection for data on-premises, in remote systems, in private and public clouds, and on mobile devices. It features Acronis Active Protection™ for proactive protection against ransomware, enhanced backup validation, and blockchain-based authentication of backups via Acronis Notary™.

It enables protection of any workload, including both on-premises, as well as AWS and Microsoft Azure clouds. For hypervisors, Acronis supports VMware vSphere, Microsoft Hyper-V, Linux KVM, Citrix XenServer and Red Hat Virtualization. For OS’s, Acronis supports Microsoft Windows, Linux and mac. For databases it supports Oracle, Exchange, SQL Server, SharePoint and SAP HANA.

Acronis Cyber Backup also supports protection of Office 365 and Google G Suite. The backups are stored in the Acronis Cloud Storage.

Acronis’s cyber protection solution should be considered by organizations that require a solution that includes protection for Microsoft Office 365 as well as a comprehensive DRaaS.
Strengths

- Mature product with strong customer base
- Support for wide range of databases and applications
- Support for VM Ware and Hyper-V protection
- Protection for Office 365 and G Suite
- Integrated deduplication
- Innovative blockchain based backup protection.
- Included ransomware protection

Challenges

- Limited support for other cloud services for storage
- No support for other cloud services for DR hot standby
5.2 Actifio

Actifio is a privately held organization with headquarters in Waltham Massachusetts in the USA. Actifio Enterprise Data as a Service (EDaaS) captures application data directly from the application and manages it on any chosen infrastructure. Data, governed by user-defined SLAs, is available whenever and wherever needed to support the enterprise. Actifio’s Virtual Data Pipeline™ (VDP) virtualizes data with data protection and access for backup and restore, test and development, analytics, disaster recovery and business continuity all through a single storage platform. Actifio’s software is delivered either as a physical appliance, CDS, or a virtual appliance, Sky. Sky is delivered as a virtual machine image that runs locally in VMware or Hyper-V environments using existing customer storage. Sky can also run in a variety of public clouds including Amazon AWS, Microsoft Azure and Oracle Cloud.

It enables protection of a broad range of platforms premises as well as in cloud. For hypervisors, Actifio supports VMware and Hyper-V. For OS’s, Actifio supports Microsoft Windows, Linux (RHEL, SLES), and Unix (HP-UX, AIX, Solaris). For databases it supports Oracle, Microsoft SQL Server, SAP HANA, as well as NoSQL, MongoDB, and others. It does not support protection of SaaS such as Office 365. Actifio depends upon partners to provide DR as a managed service.

Actifio’s data protection solution is based on its innovative Virtual Data Pipeline and should be considered by organizations that wish to exploit the wider benefits that this can deliver.
Security
Interoperability
Usability
Deployment
Basic Protection
On-Premises
IaaS
SaaS
Disaster Recovery

**Strengths**
- Innovative data copy management approach
- Support for wide range of databases and applications
- Support for VM Ware and Hyper-V protection.
- Integrated deduplication
- Instant mount provides fast recovery without copying large amounts of data
- Wide choice of cloud for backup storage and disaster recovery
- Actifio GO coverage of Office 365

**Challenges**
- Limited market presence outside of North America
- Dependence on partners to deliver managed DR
5.3 Arcserve

Arcserve is a global company with headquarters in Eden Prairie, Minnesota in the USA. It has a primary focus on data backup and disaster recovery solutions. 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 private company under the ownership of Marlin Equity Partners. This report covers Arcserve Unified Data Protection (UDP) 7.0. 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.

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.

Arcserve UDP 7.0 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. It is likely to be of interest to organizations where SaaS protection is not high priority.
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
- Arcserve UDP Cloud Direct provides direct-to-cloud backup and disaster recovery as a service

Challenges

- No inbuilt functionality to detect sensitive data in backups
- No inbuilt functionality to identify selected personal data in backups
- No coverage of SaaS services except for Microsoft Office 365
- Backup to cloud requires an on-premises server
5.4 Amazon Web Services

In January 2019, AWS acquired CloudEndure and Israeli company that was previously an AWS partner. CloudEndure offers Disaster Recovery and Migration Software-as-a-Service (SaaS) solutions into Amazon Web Services (AWS). Both solutions are powered by CloudEndure’s workload mobility technology, which continuously replicates applications from physical, virtual, or cloud-based infrastructure to a low-cost “staging area” that is automatically provisioned in the customer’s chosen AWS Region. During failover, cutover, or testing, an up-to-date copy of applications can be spun up on demand and rapidly be fully functional.

CloudEndure Migration supports migration to AWS from on-premises environments, including physical and virtual infrastructure, all private clouds, and public clouds including Microsoft Azure, Google Cloud Platform (GCP), OpenStack, Oracle Cloud, CloudStack, and IBM Cloud as well as from another AWS account or AWS Region. It covers a wide range of workloads and data including databases such as Microsoft SQL Server, Oracle, and MySQL, and enterprise applications such as SAP. Continuous Data Replication takes place in the background and ensures that data is synced in real time. When cutover is initiated, CloudEndure executes an automated machine conversion and orchestration process that allows applications and databases to run natively in AWS in a short period of time.

AWS Cloud Endure provides comprehensive functionality for replication and disaster recovery based on the use of AWS. It does not support other clouds for storage, and it does not support data protection for SaaS. It should be considered by organizations that can accept these limitations.
**Strengths**

- Comprehensive replication and DR capabilities
- Comprehensive coverage of major databases and applications
- Covers on-premises workloads as well as all major cloud workloads
- Covers a wide range of VM types and hypervisor technologies
- Useful for migration as well as DR
- Supports hot standby enabling rapid service cutover

**Challenges**

- Only supports AWS as the storage / DR environment
- No inbuilt functionality to detect sensitive data in backups
- No inbuilt functionality to identify selected personal data in backups
- No coverage of SaaS services except for Microsoft Office 365
- Depends upon partners to deliver fully managed DRaaS
5.5 Cobalt Iron

Cobalt Iron is a private company with headquarters in Lawrence, Kansas in the USA. Its focus is on smart secure and automated data backup and disaster recovery. It was founded in 2013. This report covers Cobalt Iron Compass. This provides enterprise backup functionality as a SaaS solution.

The Compass™ architecture comprises 3 major components – Commander, Analytics Engine and Accelerator. Commander provides a single pane of glass web dashboard, while the Analytics Engine delivers the intelligence and insight. The Accelerator is a converged, integrated, and scalable enterprise data protection system that is constantly maintained and updated. The Analytics Engine analyses the meta data from data protection operation and provides this to the Accelerators to automate operations, avoid problems and increase efficiency.

Compass™ enables protection of a broad range of platforms including on premises, remote sites, as well as cloud services and cloud to cloud backup. Cloud services covered include Alibaba, Microsoft Azure, AWS, Google Cloud Platform and IBM Cloud. It covers Windows, Linux, Microsoft Exchange and Domino Mail, file servers, and a wide range of databases as well including Microsoft SQL, Oracle and SAP HANA, as well as VMware vSphere. Compass™ also has a virtual tape library interface that emulates tape libraries, tape drives, and tape cartridges. Built natively into Compass™ is a high level of security including encryption as well as cyber-attack protection. It should be considered by organizations looking for a SaaS based solution to simplify their backup processes.
**Strengths**

- Consolidated view for large organization with multiple sub-orgs. Built in multi-tenancy capabilities
- Innovative solution using automation and analytics to improve efficiency
- SaaS solution with option for on-premises, remote site, public, private and hybrid cloud deployment models
- On premises to cloud as well as cloud to cloud backup and replication
- Comprehensive functionality covers multiple use cases and workloads including all the common hypervisors
- Through analytics driven automation, Compass™ reduces up to 90% of daily operational tasks associated with backup
- Integration with a range of third-party orchestration and integration tools
- Strong security features

**Challenges**

- No inbuilt functionality to detect sensitive data in backups
- No inbuilt functionality to identify selected personal data in backups
- Limited protection of SaaS services
- No automation of recovery processes
5.6 Commvault

Commvault is a publicly traded data protection and data management software company headquartered in Tinton Falls, New Jersey in the USA. Commvault was formed in 1988 as a group within Bell Labs, and in 1996, it was incorporated as an independent company.

Commvault Complete™ Backup & Recovery provides backup and recovery and is one of several products that include: Commvault HyperScale™ for hyperscale scale-out, Commvault Orchestrate™ for end-to-end data syncing for faster disaster recovery, and workload migration, and Commvault Activate™ provides insight into data for data governance and compliance.

As well as providing standard backup and recovery functionality to store protected data on tape/disk media, including deduplication and encryption capabilities it can store protected data with common cloud storage providers (Amazon, Microsoft, Google and more). It fully supports all file systems, applications, databases and virtualization platforms. It also provides protection for endpoints as well as Google Apps and Database, Microsoft Office 365 and Salesforce.com. Partners provide managed services for DR.

It includes a high level of security including encryption as well as cyber-attack protection. It should be considered by organizations looking for a comprehensive solution for backup of their hybrid IT environment.
Security
Interoperability
Usability
Deployment
Basic Protection
On-Premises
IaaS
SaaS
Disaster Recovery

Strengths

• Mature solution with strong existing user base
• Comprehensive functionality covers multiple use cases
• Range of solution delivery options
• On premises to cloud as well as cloud to cloud backup
• Coverage of wide range of virtualization platforms
• Protection for Big Data apps like Hadoop
• Enhanced capabilities with machine learning
• Strong security features

Challenges

• Requires multiple products for fully comprehensive functionality
• Dependence on partners to deliver managed DR
• Lack of independent compliance certification of the solution
5.7 Dell EMC

Dell Technologies is a multinational corporation with headquarters in Round Rock, Texas. Dell EMC solutions include servers, data storage, data protection, networking and information security. This report focuses on the Dell EMC Data Protection Suite which includes NetWorker, Avamar and PowerProtect Data Manager.

Dell EMC Data Protection Suite provides a software-defined solution to protect workloads at the edge to core to cloud. It provides flexible deployment options that cover backup and recovery, disaster recovery, point-in-time recovery as well as long-term retention. It integrates with the Dell EMC PowerProtect DD Series Appliances (next generation of Data Domain) to deliver backup, replication, recovery, instance access and restore, search and analytics, and seamless VMware integration.

It provides application consistent protection for leading and emerging databases and applications using native interfaces. It enables protection of a broad range of platforms, including: Windows, Linux, Amazon EC2, Microsoft Azure, Microsoft Exchange, MS SQL, file servers, Microsoft IIS, Microsoft Active Directory, Oracle Database, PostgreSQL, VMware vSphere (agentless), Microsoft Hyper-V (agentless) and Nutanix AHV. Office 365 backup is provided through a partner (Kaseya Spanning).

Dell EMC Data Protection Suite 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. It should be considered by organization needing protection for a hybrid IT environment.
Strengths
- Mature product with strong user base
- Comprehensive functionality covers multiple use cases
- Mature architecture for hybrid protection
- Integrated encryption and deduplication
- Wide choice of cloud for backup storage and disaster recovery

Challenges
- Depends upon a partner for protection of coverage of SaaS services
- Several components are required in order to provide comprehensive protection
- Comprehensive but can get complex based on requirements
5.8 IBM

IBM offers a wide range of public and private cloud services as well as software, hardware, consulting and management services. This report focuses on the IBM’s backup offering which is IBM Spectrum Protect Plus which has its origins in Tivoli Storage Manager. IBM Spectrum Protect Plus is available as an IBM® Cloud for VMware Solutions service on IBM Cloud. It supports a range of protection storage options including IBM Cloud, AWS and Microsoft Azure.

IBM Spectrum Protect Plus provides recovery, replication, reuse, and retention for VMs, databases, and applications in hybrid multi-cloud environments. The solution can be deployed as a virtual appliance and the agentless architecture makes it easy to maintain. SLA-centric policy workflows automate the data protection lifecycle, including operational data recovery, data replication and data retention. Role-based access control (RBAC) and application integration enable self-service data reuse to improve the speed and efficacy of analytics, development, testing, and reporting.

In addition, although this is strictly out of the scope of this report, IBM DRaaS delivers a fully managed service helping businesses to reduce costs using IBM’s resiliency expertise. IBM DRaaS provides end-to-end integrated services using private, public or hybrid cloud.
## Strengths
- Mature product with extensive user base
- Full BaaS (Backup as a Service) with options supported by IBM Resiliency
- Comprehensive functionality
- Integrated encryption and deduplication
- Integration with IBM Cloud, AWS and Azure storage
- Attested security and compliance of IBM Cloud storage
- Cloud storage in a range of geographies
- Strong customer base

## Challenges
- Only supports protection for Office 365 through partners
- No protection for other important SaaS
- No integration with Google Cloud Platform
5.9 iland

iland is a global cloud service provider for infrastructure (IaaS), disaster recovery (DRaaS), and backup as a service (BaaS). Its headquarters are in Houston, Texas, with offices in London, UK, and Sydney, Australia. Its cloud services are based on VMWare and are delivered from its data centres throughout North America, Europe, Australia, and Asia. These data centres are used to hold the data backed up by the iland backup and disaster recovery services, in addition to private and public cloud IaaS.

iland Secure DRaaS allows IT workloads to be replicated from virtual or physical environments to iland’s cloud infrastructure. The services are used with tools from partners to cover a range of use cases. These include working with Zerto for on-premise virtual workloads, with Veeam for customers of on-premises Veeam Availability Suite, with VMware for native support of virtual environment in the cloud with VMware vCloud Availability and Veeam Cloud Connect backup, with Double-Take, for physical workloads and DR for other clouds. In addition, iland Secure Cloud-to-Cloud Recovery?, covers DR needs between iland clouds.

It provides a range of DR service options from fully assisted to do-it yourself with support from run books and tooling. Through Zerto it offers flexibility, customized runbook functionality, optimized RPOs and near-zero RTOs. It has excellent overall functionality, but with somewhat limited coverage of SaaS, through partnerships. It should be considered by organizations wanting a full DRaaS offering and are prepared to use the iland cloud as the storage for the backups and DR.
Strengths
- Full service DRaaS with options and tooling
- Comprehensive functionality through partnerships covers multiple use cases
- Optimized RPOs and near zero RTOs
- Integrated encryption and deduplication
- Attested security and compliance of cloud storage
- Cloud storage in a range of geographies
- Strong customer base

Challenges
- Only supports iland cloud as backup storage
- Dependent upon partners to provide some functionality
- Limited coverage of SaaS
5.10 Micro Focus

Micro Focus is a global infrastructure software business with revenues of over $4.7B in 2018. In 2017 Micro Focus closed the deal to acquire HPE software business and, as part of this acquisition, obtained HPE Data Protector backup and disaster recovery solution which is now sold as Micro Focus Data Protector.

Micro Focus Data Protector is offered in two editions: Data Protector Premium which supports hybrid environments (virtual and physical), and Data Protector Express designed for backup and restore of virtual environments. The Premium edition provides a standardized approach to data protection across a wide range of physical and virtual environments, operating systems, applications and databases. It enables data to be backed up to disk, tape and cloud services. It features deep integration with both physical and cloud storage technologies ensuring efficient use of resources as well as rapid recovery. However, protection of data in SaaS clouds such as Microsoft Office 365 is an important feature that is currently missing.

Micro Focus Data Protector is a mature product with comprehensive functionality and a strong user base. It has a multi-tiered architecture that enables centralized management and control of data protection across physical, virtual and cloud environments. Organizations where their hybrid IT protection requirements do include SaaS environments should include this on their shortlist of products for consideration.
Strengths

- Mature product with strong user base
- Comprehensive functionality covers multiple use cases
- Integration with VM Ware and Hyper-V for virtual server protection
- Integration with leading DBMS and business applications for consistent protection
- Integration with storage arrays for rapid recovery and efficiency
- Choice of cloud as a backup storage tier
- Strong security features

Challenges

- No support for protecting data in SaaS clouds
- No inbuilt functionality to detect sensitive data in backups. This requires the use of other Micro Focus products
- No inbuilt functionality to identify selected personal data in backups
5.11 Microsoft

Microsoft is a global provider of cloud, infrastructure and software services. Microsoft Azure is their IaaS offering and in June 2018, Microsoft announced the general availability of Azure Site Recovery to replicate and protect IaaS based applications running on Azure.

Microsoft Azure Site Recovery is a disaster recovery as a service (DRaaS) that is provided through the Microsoft Azure Service Portal. It uses Azure Backup to backup data from on-premises machines, and Azure VMs. Azure Site Recovery enables the user to replicate machines from a primary location to a secondary one. This makes it possible for the service to continue from the secondary location when the machines in the primary location are not available. Using Azure Backup, data can be backed up and recovered at a granular level, including backup of files, folders, machine system state, and app-aware data backup. This also provides protection for a range of industry leading DBMS including SQL Server, Oracle and SAP HANA.

Azure Site Recovery is a self-service offering; however, Microsoft partners offer managed DRaaS services based on it. It covers physical servers, Azure VMs and VMware VMs. The protected data can only be stored in Azure, albeit with a choice of regions. There is no coverage of data held in SaaS or in other vendors IaaS. This should be considered by organizations using Azure and their main IaaS provider and where their hybrid IT protection requirements do include SaaS environments.
### Strengths

- Easy to implement within the scope of the environments covered
- Deep integration with Azure
- Continuous replication for Azure VMs; and VMware VMs Integration with VM Ware and Hyper-V for virtual server protection
- Granular protection through Azure Backup
- Integration with leading DBMS and business applications
- Support for testing of DR plans without affecting running services
- Strong security features

### Challenges

- No support for data held in other vendors’ clouds
- No support for protecting data in SaaS clouds
- No data deduplication but only changed data is copied
- No inbuilt functionality to identify selected personal data in backups
5.12 Rubrik

Rubrik is a multi-cloud data control company based in Palo Alto, California, USA that was founded in December 2013. Rubrik Cloud Data Management provides single platform to manage all data in the cloud, at the edge, or on-premises for backup, disaster recovery, archival, compliance, analytics, and copy data management.

Rubrik is available via backup appliances or software only for deployment on either certified customer hardware or in the cloud. Customers can deploy Rubrik in the cloud and can use Polaris for cloud native protection of AWS and Azure (while ingesting metadata into their federated data management platform). Its solution can protect enterprise applications, search across applications and files, and spin up test/dev instances in the cloud. In addition to supporting live mount of VMs, SQL and Oracle databases for instant recovery, it enables enterprises to leverage the public cloud to recover in the event of a disaster, to migrate data across data centres and clouds, and protect cloud-native applications.

It supports a wide range of physical servers, NAS and DBMS including Oracle, SQL Server, MySQL, PostgreSQL and SAP HANA as well as MongoDB and Cassandra. It also covers virtual environments including VMWare, Hyper V and Nutanix. It supports applications in Azure, AWS and GCP, Oracle Cloud as well as Office 365 through Polaris. Protected data can be tiered to Azure, AWS, GCP. It provides a high level of security with encryption as standard and support for MFA. As well as supporting self-service DR through a rich set of APIs, it also allows customers to gain insights into protected data via Polaris, Radar or Sonar. Radar facilitates recovery from ransomware and Sonar helps with compliance. Its coverage of SaaS is limited to Office 365. Rubrik’s appliance and software offerings have been certified to EAL2+ of the Common Criteria for Information Technology Security Evaluation and Rubrik claims ISO/IEC 27001 certification and SOC 2 attestation of their services although this is not yet publicly announced. Rubrik should be considered by organizations with a hybrid IT deployment and limited need for SaaS protection.
Strengths

- Comprehensive functionality covers multiple use cases
- Supports VMWare and Hyper-V for virtual server protection
- Integration major DBMS and business applications
- Strong support for MySQL commonly used by cloud native apps
- Strong support for IaaS based workloads
- Choice of cloud as backup storage
- API based approach
- Strong security features

Challenges

- Support for SaaS protection limited to Office 365
- Independent certification of services claimed but not yet published
- Managed DRaaS provided through partners
5.13 Unitrends

Unitrends was acquired by Kaseya, with headquarters in Miami Florida in the USA, during 2018. Unitrends offers a variety of backup and disaster recovery solutions that include coverage for on-premises, cloud apps and SaaS with a range of storage options including public cloud.

Unitrends backup solutions are available as Recovery Series all-in-one appliances or Unitrends Backup software, a pre-packaged virtual appliance. Both Unitrends Recovery Series appliances and Unitrends Backup software offer fully integrated backup, replication, deduplication, archiving, and instant recovery. It can run on VMware vSphere, Microsoft Hyper-V, or XenServer or be deployed as a virtual machine (VM) within the Microsoft Azure or Amazon Web Services cloud. Unitrends Direct to Cloud Backup can protect laptops, PCs and other endpoints connected to the corporate network. It can be used alone or to complement the Unitrends all-in-one backup appliance. Unitrends also offer Spanning Backup for Office 365 this provides protection for with automated backup including unlimited storage and point-in-time, granular restore of mail, calendar, OneDrive, and SharePoint. in March 2020, Spanning launched Dark Web Monitoring for Office 365, an add-on for its Spanning Backup for Office 365 product to provide an additional layer of protection.

Unitrends Disaster Recovery as a Service provides enables launching applications in the Unitrends Cloud to continue to operate during a disaster or outage. “Included with all DRaaS service levels is a White Glove Service”, where Unitrends customer support will help recover from disaster and rebuild your on-premises site. The Unitrends Cloud is compliant with some industry regulations, such as SSAE 18 (SOC 2), HIPAA, CJIS, and GDPR. It should be considered by organizations with a hybrid IT deployment and need for Office 365 protection.
Strengths

- Comprehensive functionality covers multiple use cases
- Supports VMWare and Hyper-V for virtual server protection
- Integration major DBMS and business applications
- Support for AWS and Azure based workloads
- Protection for Office 365, G Suite and Salesforce
- Choice of cloud as backup storage
- DRaaS offering including planning tools

Challenges

- Support for SaaS protection limited to Office 365 G Suite and Salesforce
- No integration with snapshots from primary storage
5.14 Veeam

Veeam Software is a privately held company that was founded in 2006 and was acquired in 2020 by Insight Partners. It develops and sells backup, disaster recovery and intelligent data management software for virtual, physical and multi-cloud infrastructures. This report focuses on Veeam Availability Suite 10 which was released in February 2020.

Veeam Availability Suite 10 comes in a several editions of which Enterprise Plus provides the most comprehensive functionality. It provides protection for virtual, physical and cloud-based workloads. It features a single management console from which to manage backup, recovery and replication of all applications and data. Its Cloud Tier enables long term data retention by using native object storage integrations with Amazon S3, Azure Blob Storage, IBM Cloud Object Storage, as well as S3-compatible service providers and on-premises storage solutions. Veeam DataLabs Staged & Secure Restore functionality helps with GDPR by streamlining “right to be forgotten” requests and reduce security risks by automatically scanning and verifying backups after malicious attacks. While it supports data protection for Microsoft Office 365 it does not cover Google G-Suite and other SaaS services such as Salesforce. It does not offer as wide a range of coverage as some other solutions.

Veeam Availability Suite 10 has many new features including “Multi-VM Instant Recovery” and “ransomware-proof backups with S3 object lock”. Following the recent acquisition, it is now a US based company which retains its large European presence in terms of customers as well as R&D and Marketing. It provides specific tools to help with GDPR compliance. It should be considered by organization needing the specific protection features it provides.
Strengths

- Mature product with strong user base
- Comprehensive functionality covers multiple use cases
- Integration VMware and Hyper-V for virtual server protection
- Multi-VM Instant recovery and ransomware proof backups
- Integration with some DBMS and business applications
- Includes support for cloud-based workloads and Office 365
- Tools to help with GDPR compliance
- Choice of cloud as a backup storage

Challenges

- The range of protected platforms is less comprehensive than some competitive products
- The range of supported IaaS and PaaS cloud services for backing up data is less comprehensive than some competitive products
- Does not provide protection for many popular SaaS
- DRaaS provided through partners
5.15 Veritas

Veritas is a global business with headquarters in the USA and an annual revenue of over $2 Billion. In 2014 Veritas was demerged from Symantec and is now owned by the Carlyle Group. It has a focus on helping its customers to discover and protect their data. This report focuses on Veritas NetBackup™ 8.2.

Veritas NetBackup provides backup and recovery of business data across hybrid, physical, virtual and multi-cloud environments. It scales to support large workloads and delivers capabilities for virtualized and cloud-based deployments. It supports a wide range of environments and integrates with every layer of the infrastructure stack. NetBackup integrates with hypervisors including VMware vSphere®, Microsoft® Hyper-V, Nutanix AHV, Red Hat Virtualization and OpenStack. It integrates with relational database and application platforms, including IBM DB2®, Microsoft® Exchange Server, Microsoft SQL Server®, MySQL™, Oracle®, SAP® and others. It supports data protection for Microsoft Office 365, Google G-Suite and Salesforce SaaS services. It supports third-party cloud storage providers such as AWS, Microsoft® Azure and Google that can be incorporated into NetBackup policies. With NetBackup CloudCatalyst, backup data is deduplicated before being transferred and stored within the cloud.

Veritas NetBackup 8.2 is a leading product with comprehensive functionality and a strong user base. Organizations with a hybrid IT environment (including IaaS as well as the range of SaaS services covered) looking for a data protection solution should include this on their shortlist of products for consideration.
Security
Interoperability
Usability
Deployment
Basic Protection
On-Premises
IaaS
SaaS
Disaster Recovery

Strengths

- Mature product with strong user base
- Comprehensive functionality covers multiple use cases
- Integration with wide range of hypervisors for virtual server protection
- Integration with leading DBMS and business applications
- Includes support for cloud-based workloads and some SaaS
- Choice of cloud as a backup storage

Challenges

- Missing functionality to identify compliance related data you need to use Veritas Information Studio
- Mostly requires the deployment of agents
- Need to fully integrate recently acquired APTARE IT Analytics
6 Related Research

Advisory Note: Security Organization, Governance, and the Cloud – 71151
Advisory Note: Cloud Provider Assurance – 70586
Advisory Note: Selecting your cloud provider – 70742
Advisory Note: Rising to the Security Challenge of Heavy Cloud Adoption - 72542
Leadership Brief: Cloud Provider Codes of Conduct and GDPR - 70276
Leadership Brief: Six Key Actions to Prepare for GDPR - 70340
Executive View: SAP HANA Enterprise Cloud – Security and Compliance - 71117
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
- Functionality
- Ease of Delivery
- Interoperability
- Usability

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.

**Ease of Delivery** 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.

We focus on security, functionality, ease of delivery, interoperability, and usability 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.
Content of Figures

Figure 1: Market Trends
Figure 1: Disaster Recovery Market Trend from traditional tools to cloud based services
Figure 3: Featured for Innovation
Figure 4: Featured for SaaS Protection
Figure 5: Featured for Comprehensive Capabilities
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 back 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.