Cloud Backup for Ransomware Protection

Mike Small

March 30

LEADERSHIP COMPASS 2023

Introduction / Executive Summary

The KuppingerCole Leadership 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 Leadership Compass covers solutions that …

> Provide backup, restore, and disaster recovery of all data held in today’s hybrid IT services into the cloud. It provides an assessment of the capabilities of these solutions to meet the backup and disaster recovery needs of organizations with a particular focus on ransomware protection.

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 a growing market offering enterprise BaaS (Backup as a Service) and DRaaS (Disaster Recovery as a Service).

A major threat to business continuity is ransomware. This is because organizations are now very dependent upon their IT services and the data they contain. Working from home has increased the risks of ransomware because of the lack of data protection for unmanaged end user devices. In addition, cyber adversaries have made ransomware protection more difficult by attacking the backup processes as well as the backed-up data itself.

Most of the existing vendors are adapting their solutions to this hybrid service delivery model, but there is still some way to go, especially around SaaS platforms. In addition, new vendors, including the cloud service providers themselves, now offer solutions to protect data in their cloud and to store backup data from other sources. For SaaS, most vendors now offer solutions for customers to back-up the data held in Microsoft Office 365. Some offer solutions that also cover Google Workspace and Salesforce, however, there is a lack of comprehensive coverage for data in other SaaS platforms. This is likely to become more of a problem with the increase in the variety of business solutions delivered as SaaS.

Customers should look for solutions that provide capabilities that align with their business requirements for service continuity. Organizations must identify their business-critical systems and data and use this to define the business continuity protection needed. This sets the recovery objectives for backup and disaster recovery processes and tools.

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

- Data is the most important business asset of the modern organization, and it needs to be protected against unauthorized access as well as ransomware and loss.
- Today's e-commerce, financial services, and critical infrastructure demand continuous availability where even seconds of downtime could lead to severe damage and disruption.
- Ransomware is a major threat to business continuity. Cyber adversaries use various techniques to infiltrate an organization's IT systems and make changes that prevent the organization from accessing their data and using their IT services.
- Backup and Disaster Recovery tools provide important controls that are needed to recover data and restore services following cyber-attacks. They are an essential part of a complete information lifecycle protection approach.
- Today's hybrid IT environment creates additional challenges for backup and disaster recovery because of its complexity and heterogeneity.
- Traditional backup tools deployed as a combination of software, agents and appliances are complex to use, difficult to manage, hard to secure, and are often compromised as part of a ransomware attack.
- Cloud services create new backup and DR challenges. Organizations can misunderstand the shared responsibility model and believe data protection is the sole responsibility of the cloud provider. In addition, Big Data and massive data lakes held in cloud services create additional data resilience challenges.
- Cloud services also provide a way to overcome these challenges. Software as a Service removes many of the management and security tasks from the end user. They provide highly resilient and immutable storage capabilities to protect backup data. They also enable highly scalable backup solutions using modern architectures.
- The Overall Leaders (in alphabetical order) are Arcserve, Cohesity, Commvault, Druva, OpenText (Micro Focus), Veeam® and Veritas.
- The Product Leaders (in alphabetical order) are 11.11 Systems, Arcserve, Cobalt Iron, Cohesity, Commvault, Druva, OpenText (Micro Focus), Veeam®, and Veritas.
- The Innovation Leaders (in alphabetical order) are Clumio, Cobalt Iron, Cohesity, Commvault, Druva, HYCU, and Veeam®.
- The Market Leaders (in alphabetical order) are Arcserve, Commvault, OpenText (Micro Focus), Veeam®, and Veritas.
- The Market Disrupters (in alphabetical order) are Cobalt Iron, Clumio, Druva, and HYCU. These innovators are setting new standards for cloud backup solutions in this market by providing easy to use, lightweight and highly scalable SaaS based solutions.

Market Segment

Data is the most important business asset of the modern organization, and it needs to be protected against unauthorized access as well as ransomware and loss. Organizations are using cloud services to improve flexibility, to create new products and to reduce costs through digital transformation. This is creating a tension between the benefits that cloud services provide and the risks that using a third party, often in another country, to process data create.

It is important to remember that information protection must cover the whole of the information lifecycle and requires a wide range of different types of controls. Backup and Disaster Recovery tools provide some but not all of the controls that are needed. The KuppingerCole Information Protection Life Cycle (IPLC) and Framework[1] describes the phases, methods, and controls associated with the protection of information. Though other IT and cybersecurity frameworks exist, none specifically focus on the protection of information across its use life. The IPLC documents three stages in the life of information and six categories of controls which can be applied to secure information.

Figure 1 illustrates the role of cloud backup and disaster recovery in the information protection lifecycle.

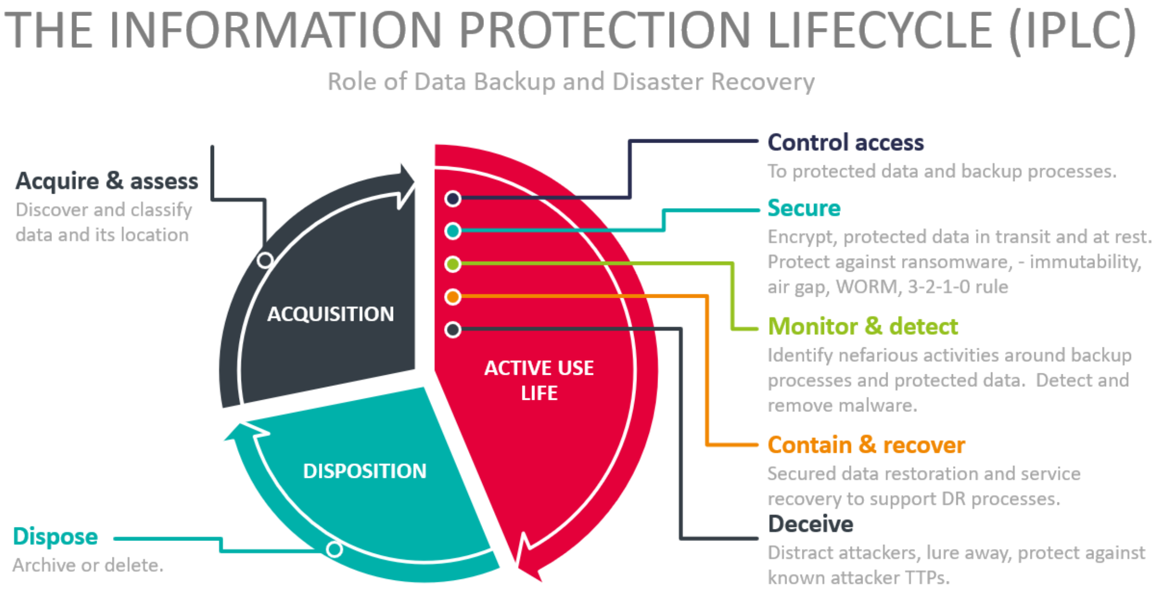

THE INFORMATION PROTECTION LIFECYCLE (IPLC)
Role of Data Backup and Disaster Recovery
Acquire & assess
Discover and classify data and its location
ACQUISITION
ACTIVE USE LIFE
DISPOSITION
Dispose
Archive or delete.
Control access
To protected data and backup processes.
Secure
Encrypt, protected data in transit and at rest. Protect against ransomware, - immutability, air gap, WORM, 3-2-1-0 rule
Monitor & detect
Identify nefarious activities around backup processes and protected data. Detect and remove malware.
Contain & recover
Secured data restoration and service recovery to support DR processes.
Deceive
Distract attackers, lure away, protect against known attacker TTPs.

Figure 1: The Role of Backup and Disaster Recovery tools in the Information Protection Lifecyle

The term “Cloud Backup” stands for a comprehensive set of software, and services that protect business critical data held by organizations on-premises and in cloud services

[1] Leadership Brief: The Information Protection Life Cycle and Framework: Secure

against ransomware and other risks by taking copies of that data and providing capabilities to restore it and the services.

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 are backed up in a way that allows them to be restored following unwanted events such as ransomware attacks as well as physical and logical damage to the storage devices or to the IT installation.

Today, ransomware is a major threat to business continuity. Cyber adversaries use various techniques to infiltrate an organization’s IT systems and make changes that prevent the organization from accessing their data and using their IT services. The organization then faces the choice of either paying a ransom to regain access or restoring the affected services and data from backups. Cyber adversaries attempt to make restoration and recovery more difficult by attacking the backup processes as well as the backed-up data.

Making backup copies of data is necessary but not sufficient, and organizations need to be able to use the backed-up data to recover their services. This can be a complex process and the backup processes must take account of the need to recover. Cloud Backup solutions must include the capabilities and services needed to recover data and rapidly restore services.

Two parameters specify the objectives for business continuity supported by Cloud Backup solutions. RPO (Recovery Point Objective) – this defines how frequently data must be backed up. RTO (Recovery Time Objective) – this defines how long it should take to recover from an incident.

The time criticality of digitized business services increases the need for an always on IT service architecture. Today’s e-commerce, financial services, and critical infrastructure demand continuous availability where even seconds of downtime could lead to severe damage and disruption. An always on architecture depends upon replicated service components with automated failover to ensure business continuity when individual elements fail.

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

Delivery Models

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

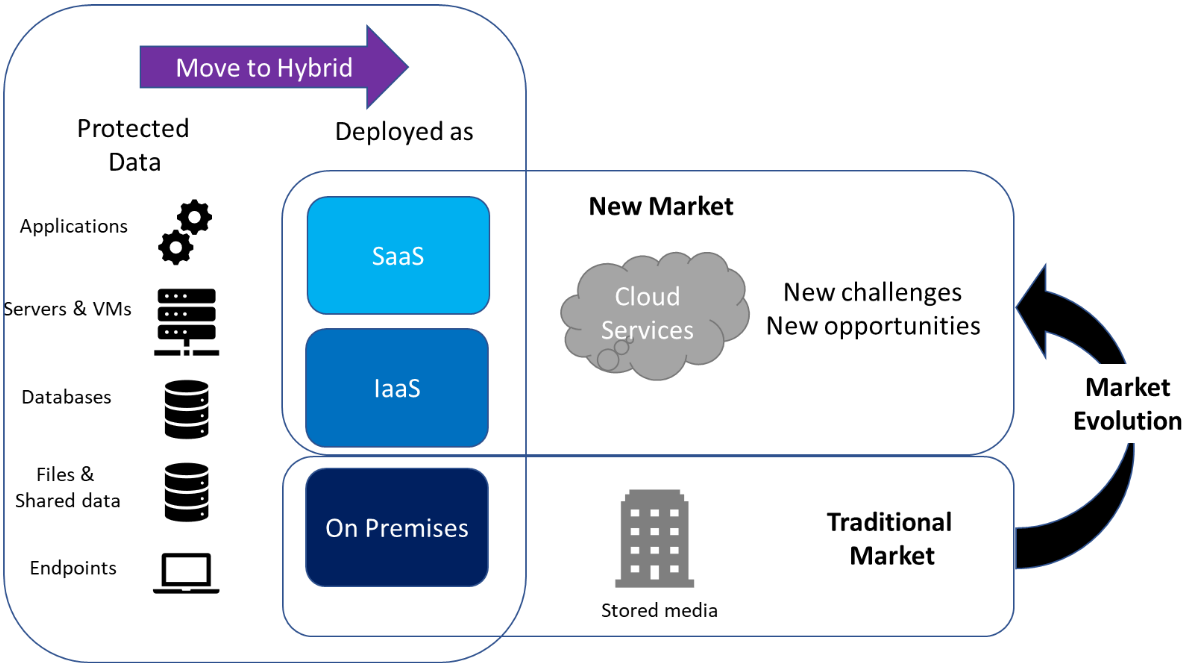


Figure 2: Evolution of Backup and Disaster Recovery

Most organizations now have a hybrid IT environment with IT services delivered in multiple ways, some remaining on-premises and others delivered as cloud services. This adds to the complexity of backup, restoration, and recovery processes.

The cloud also provides an alternative location for backup data since major cloud services are delivered from highly secured datacenters in multiple geographic locations. Organizations can therefore use the cloud to store their backup data with a high degree of resilience and this also reduces the delays and risks previously involved in the physical transfer of media to secure locations.

There is a temptation to believe that the use of a cloud service removes the need for the customer to consider the resilience of their data. The responsibility for data held in cloud services is shared between the tenant and the service provider and there are many situations where the tenant is responsible for the resilience of their data. In addition, where multiple data protection solutions are used this increases the management burden. To avoid this, organizations should look to implement a single solution that covers all the different use cases.

The cloud also provides an opportunity to simplify the delivery of backup and disaster recovery as SaaS. This eliminates the many tasks involved in managing, administering, and securing the backup services, software, and appliances. Modern architectures such as containerization and serverless also provide increased scalability and flexibility in the solutions.

These processes and tools can be complex, and, because of this, solutions should provide organizations with options to choose the level of managed service that is appropriate for their needs. The services on the market range from a full “white glove” managed service covering everything to self-service DRaaS providing only the tools needed.

Deployment models for Cloud Backup and Disaster Recovery include:

- As a physical appliance – that can be deployed on premises or in a data center.
- As a virtual appliance that can be deployed on-premises or in a cloud service.
- As a service from Multi-tenant public cloud services where updates and patches are deployed by the service provider across all tenants with full automation. This is a growing market because of ease of adoption combined with the scalability offered by public clouds.
- As single-tenant services that can operate in various deployment models, i.e., in private or public clouds or even on-premises, where they are operated in a full as-a-service model, i.e., services where updates, patches, etc. are deployed by the service provider across all tenants with full automation.

Required Capabilities

This Leadership Compass analyses the main attributes and functions of Cloud Backup for Ransomware Protection solutions. These capabilities should include:

- **Basic capabilities –** including data backup, data replication, data recovery, system restoration, and continuous data protection. The storage systems and data types protected by the solution. The cloud services in which user organizations can hold their protected data. How the solution supports realistic RPO and RTO targets. How the solution protects the backup data against deterioration. The way in which the solution minimizes the size of backed up data - for example through deduplication that removes multiple copies within the protected data.
- **Extended capabilities –** including support for near zero RTO and continuous replication for zero RPO. Support to automatically migrate data and applications between different environments to facilitate failover and failback. Support to non-destructively test data restoration and service recovery as well as capabilities for data archive / long-term retention.
- **Deployment** - how quickly, easily, and repeatably can the solution be deployed. The deployment options that the solution offers. Whether the solution requires agents installed on the protected systems.
- **Administration** - how easy it is to administer the solution. For example, GUI/Wizard provided for ease of use, CLI/APIs for automation. Capabilities to securely delegate administration to line-of-business managers and application owners.
- **Data Security** – the capabilities to protect backed-up data against theft, unauthorized access, and corruption. How the solution protects data in transit (for example, support for the latest versions of TLS 1.3). How the solution protects data at rest – the type of encryption the solution supports and how the solution secures the encryption keys. How the customer can manage the encryption keys.

- **Cyber Security –** How the solution is secured. Controls over administrative access including multi-factor authentication and granular authorization methods such as role-based and policy-based access control. Support for secure delegation of administration. How API and CLI access is secured against unauthorized access.
- **Ransomware Protection –** additional capabilities to protect against and recover from ransomware. For example, detection and control over abnormal administrative activities, additional protection for backed-up data (air gap, object lock, write once). Protection against malware, ransomware, and other forms of cyber-attack including proactive scanning of backups. Scanning of backed-up data to find and remove malware.
- **Disaster Recovery –** how the solution supports data recovery and service restoration - for example: run books, workflows, and process automation. Full stack restoration capabilities – (i.e., the coordinated restoration of multiple service components). DRaaS (Disaster Recovery as a Service) capabilities and guaranteed SLAs for RPO/RTO.
- **On-premises Protection –** out-of-the-box protection for storage and data types. Volumes, Databases, File Systems, File shares, OS Images, Hypervisor images, email servers and other applications. The out-of-the-box capabilities to protect DBMS including MS SQL, MySQL, Oracle, SAP HANA, others. Automated capabilities to discover and snapshot environments and applications.
- **IaaS Services Protection –** out-of-the-box coverage of the IaaS services. For example, major services such as AWS, Google, IBM Cloud, and Microsoft Azure. The capabilities to protect cloud DBMS including MS SQL, MySQL, Oracle, and SAP HANA. Capabilities to protect data held in the types of storage found in IaaS services e.g., files, file systems, object storage, etc. Capabilities to snapshot and restore the native cloud service VMs. Support for replicating applications to other regions for added DR readiness.
- **SaaS Protection –** the SaaS services covered out-of-the-box. These should include major services such as Microsoft Office 365, Google Workspace, Salesforce and cover the types of data that are found in these services.
- **Regulatory Compliance –** the capabilities provided by the solution for the customer to use it in a way that complies with laws and regulations across the world. These include customer control over the geographic jurisdiction in which the protected data is held as well as over encryption and the encryption keys. Capabilities to identify and classify sensitive data within the protected data and to add extra protection for this data. Audit capabilities provided as well as independent certifications for compliance with laws and regulations across the world. Up to date certification / attestation against relevant cloud hosting and security standards such as CSA Star, ISO 27001, SOC 2 Type 2, etc. Compliance with export control regulations where applicable.

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

The Overall Leadership rating provides a consolidated view of all-around functionality, innovation, market presence, and financial position. However, these vendors may differ significantly from each other in terms of product features, platform support, and integrations. Therefore, we strongly recommend looking at all the leadership categories as well as each entry in chapter 5 to get a comprehensive understanding of the players in this market and what use-cases they support best.

Overall Leadership

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the centre, and Leaders on the right.

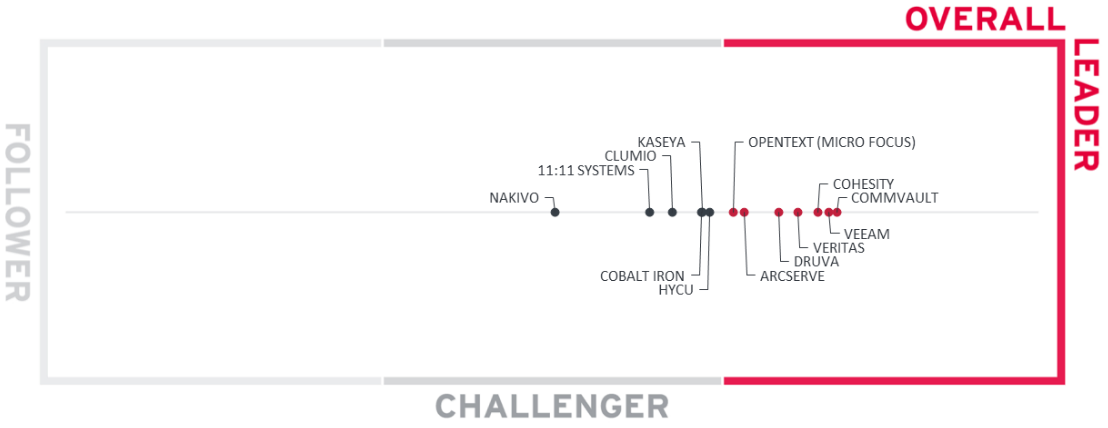


Figure 3: Overall Leadership in the Leadership Compass Cloud Backup for Ransomware Protection

The Overall Leaders are (in alphabetical order):

- Arcserve
- Cohesity

- Commvault
- Druva
- OpenText (Micro Focus)
- Veeam®
- Veritas

The Overall Challengers are (in alphabetical order): 11.11 Systems, Cobalt Iron, Clumio, HYCU, Kaseya, and Nakivo.

Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the Required Capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership Chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the centre. Followers are in the lower section.

The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership.

The vertical axis represents the market position plotted against product strength rating on the horizontal axis.

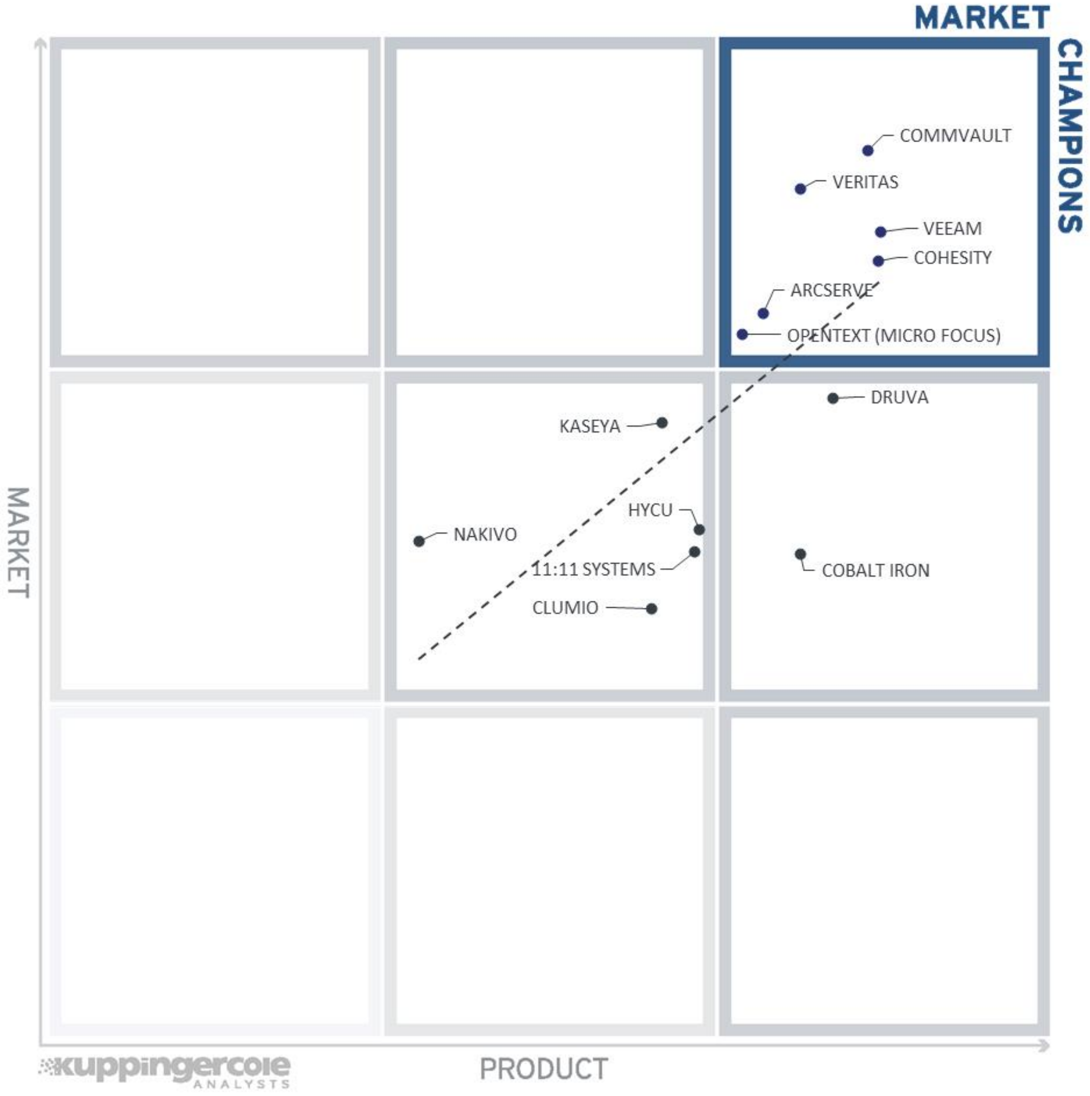


Figure 7 The Market/Product Matrix for Leadership Compass Cloud Backup for Ransomware protection

This comparison shows which vendors are better positioned in our Product Leadership analysis than their position in the Market Leadership analysis. Vendors above the line are somewhat "overperforming" in the market. It comes as no surprise that these are often very large vendors, while vendors below the line may more often be innovative but focused on specific regions as an example.

In the upper right segment, we find "**Market Champions**". Given that the backup market is mature, we see Cohesity, Commvault, Veritas, OpenText (Micro Focus), Veeam®, and Arcserve as market champions positioned in the top right-hand box.

Market Disrupters - In the middle right-hand box, we see two vendors that deliver strong product capabilities for cloud backup for ransomware protection but are not yet considered Market Champions. Cobalt Iron and Druva have a strong potential to disrupt the market and improve their market position due to the strong product capabilities they are already delivering.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not market leaders. These vendors include 11:11 Systems, Clumio, HYCU, Kaseya, and Nakivo. Clumio has a visionary approach to the emerging market for Big Data, others focus on the needs of specific markets.

Products and Vendors at a Glance

This section provides an overview of the vendors' various products we have analyzed within this KuppingerCole Leadership Compass on Cloud Backup for Ransomware Protection. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name.

Product(s) from Vendor	Security	Functionality	Deployment	Interoperability	Usability
11:11 SYSTEMS, INC.	strong positive	strong positive	strong positive	positive	strong positive
ARCSERVE	strong positive	strong positive	strong positive	strong positive	strong positive
CLUMIO	strong positive	positive	strong positive	positive	strong positive
COBALT IRON	strong positive	positive	strong positive	strong positive	strong positive
COHESITY	strong positive	strong positive	strong positive	strong positive	strong positive
COMMVAULT	strong positive	strong positive	strong positive	strong positive	strong positive
DRUVA	strong positive	strong positive	strong positive	strong positive	strong positive
HYCU	strong positive	strong positive	strong positive	strong positive	strong positive
KASEYA	positive	strong positive	positive	strong positive	positive
NAKIVO	positive	positive	positive	positive	positive
OPENTEXT (MICRO FOCUS)	strong positive	strong positive	positive	strong positive	strong positive
VEEAM®	strong positive	strong positive	strong positive	strong positive	strong positive
VERITAS	strong positive	strong positive	strong positive	strong positive	strong positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
11:11 SYSTEMS, INC.	positive	positive	positive	neutral
ARCSERVE	positive	strong positive	strong positive	strong positive
CLUMIO	strong positive	positive	positive	neutral
COBALT IRON	strong positive	positive	positive	positive
COHESITY	strong positive	strong positive	strong positive	strong positive
COMMVAULT	strong positive	strong positive	strong positive	strong positive
DRUVA	strong positive	positive	strong positive	strong positive
HYCU	strong positive	positive	positive	positive
KASEYA	positive	positive	strong positive	positive
NAKIVO	positive	positive	positive	positive
OPENTEXT (MICRO FOCUS)	positive	strong positive	strong positive	strong positive
VEEAM®	strong positive	strong positive	strong positive	strong positive
VERITAS	positive	strong positive	strong positive	strong positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For this leadership compass, we look at the following eight categories:

- **Basic Functionality –** this category measures the basic backup and disaster recovery capabilities provided by the solution. These include data backup, data replication, data recovery, system restoration, and continuous data protection. The range of storage systems and data types protected by the solution. The range of cloud services in which user organizations can hold their protected data. How well the solution supports realistic RPO and RTO targets. How well the solution protects the backup data against deterioration. How well the solution minimizes the size of backed up data.
- **Ransomware Protection –** this category measures the additional capabilities the solution provides to protect against and to recover from ransomware. For example, detection and control over abnormal administrative activities, additional protection for backed-up data (air gap, object lock, write once). Protection against malware, ransomware, and other forms of cyber-attack including proactive scanning of backups Scanning of backed-up data to find and remove malware.
- **Data Security –** this category measures the capabilities the solution provides to protect backed-up data against theft, unauthorized access, and corruption. It includes the capabilities to protect data in transit (for example, support for the latest versions of TLS 1.3) and to protect data at rest (for example, the type of encryption the solution supports and how the solution secures the encryption keys.)
- **Disaster Recovery –** this category measures the capabilities the solution provides to recover data and to restore service, for example, run books, workflows, and process automation. It includes the capabilities provided for restoration of the full-service stack (i.e., the coordinated restoration of multiple service components). It also considers the capabilities provided for DRaaS (Disaster Recovery as a Service) and the guaranteed SLAs for RPO/RTO.
- **SaaS Protection –** this category measures the capabilities the solution provides to protect data held in SaaS. It considers the range of services covered out-of-the-box. These include major services such as Microsoft Office 365, Google Workspace, Salesforce, and the types of data that are found in these services.
- **IaaS Protection –** this category measures the capabilities the solution provides out-of-the-box for IaaS services. These include the major IaaS services such as AWS, Google, IBM Cloud, and Microsoft Azure. It considers the capabilities provided to

protect cloud DBMS including MS SQL, MySQL, Oracle, and SAP HANA as well as data held in the types of storage found in these IaaS services e.g., files, file systems, object storage, etc. It also includes the capabilities provided to snapshot and restore native cloud service VMs as well as support for replicating applications to other cloud regions.

- **On-premises Protection –** this category measures the capabilities the solution provides to protect services and data on-premises and at the edge. It covers the types of storage and applications the solution supports including volumes, databases, file systems, file shares, OS Images, and hypervisor images. Applications and databases include email servers and business applications; DBMS include MS SQL, MySQL, Oracle, SAP HANA, and others. It considers the capabilities provided by the solution to automatically discover and protect these environments and applications.
- **Compliance –** this category measures the capabilities the solution provides for the customer to use it in a way that complies with laws and regulations across the world. These capabilities include the control the customer has over the geographic jurisdiction in which the protected data is held as well as over encryption and the encryption keys. It looks at the capabilities it provides to identify and classify sensitive data within the protected data and to add extra protection for this data. It considers the range of independent certifications for the solution covering compliance with laws and regulations across the world. These include up to date certification / attestation against relevant cloud hosting and security standards such as CSA Star, ISO 27001, SOC 2 Type 2, etc. It also considers compliance with export control regulations where applicable.

Arcserve – Unified Data Protection

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

Arcserve Unified Data Protection (UDP) 9, which was released in January 2023, 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 features inbuilt integration with Sophos Intercept- X Advanced for Server, providing protection against ransomware and a wide range of cyber threats. This solution targets midmarket and enterprise customers.

UDP 9 features a range of usability enhancements. These include the option of a cloud-based console for the user to manage all their Arcserve assets, new features for MSPs, support to use any S3 compatible cloud datastore as the backup destination as well as Microsoft SQL Server and Oracle database improvements.

Arcserve OneXafe, is an object-based NAS appliance that features immutable snapshots to defend against ransomware, inline deduplication, encryption at rest, and disaster recovery with WAN optimised replication as well as energy efficiency.

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

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

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

Arcserve offers a mature set of data protection solutions and has a strong user base. The solutions provide capabilities that can satisfy many use cases across organizations of different sizes from SMBs to large enterprises. The enhancements offered by UDP 9 further improve these capabilities.

Organizations looking for a mature data resiliency solution with a wide range of deployment options should consider Arcserve.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive

Table 4: Arcserve's rating

Strengths

- Mature product with strong user base.
- Comprehensive functionality covers multiple use cases.
- Supports physical, virtual, hyperconverged, and cloud environments.
- Out-of-the box protection for a wide range of databases and applications.
- Agentless VMware, Hyper-V, and Nutanix protection.
- Integrated source side global deduplication.
- Arcserve Live Migration automatically synchronizes files, databases, and applications on Windows and Linux systems on-premises, at a remote location, or in the cloud.
- OneXafe provides an energy efficient, distributed, immutable object-store using standard storage protocols.
- Support for any S3 compatible datastore as the backup destination.
- Cloud console for integrated management from anywhere.
- Wide choice of cloud service providers for backup storage and disaster recovery.
- Provides failover capabilities for on-premises servers by transferring images to the Arcserve Cloud Hybrid datacentres.
- Arcserve UDP and Appliances protect Microsoft 365 data on-premises, in addition to other workloads.

Challenges

- UDP Backup to cloud requires an on-premises server. However, Arcserve offer Cloud Direct option if that is an issue for a customer.
- Limited integration with snapshot capabilities for major cloud services.
- Does not provide out-of-the-box support for Kubernetes backup.
- No inbuilt functionality to detect sensitive data in backups.
- No independent certification of appliances or software.
- Does not support personal data requests or eDiscovery.
- Does not support tiered long-term retention capabilities.

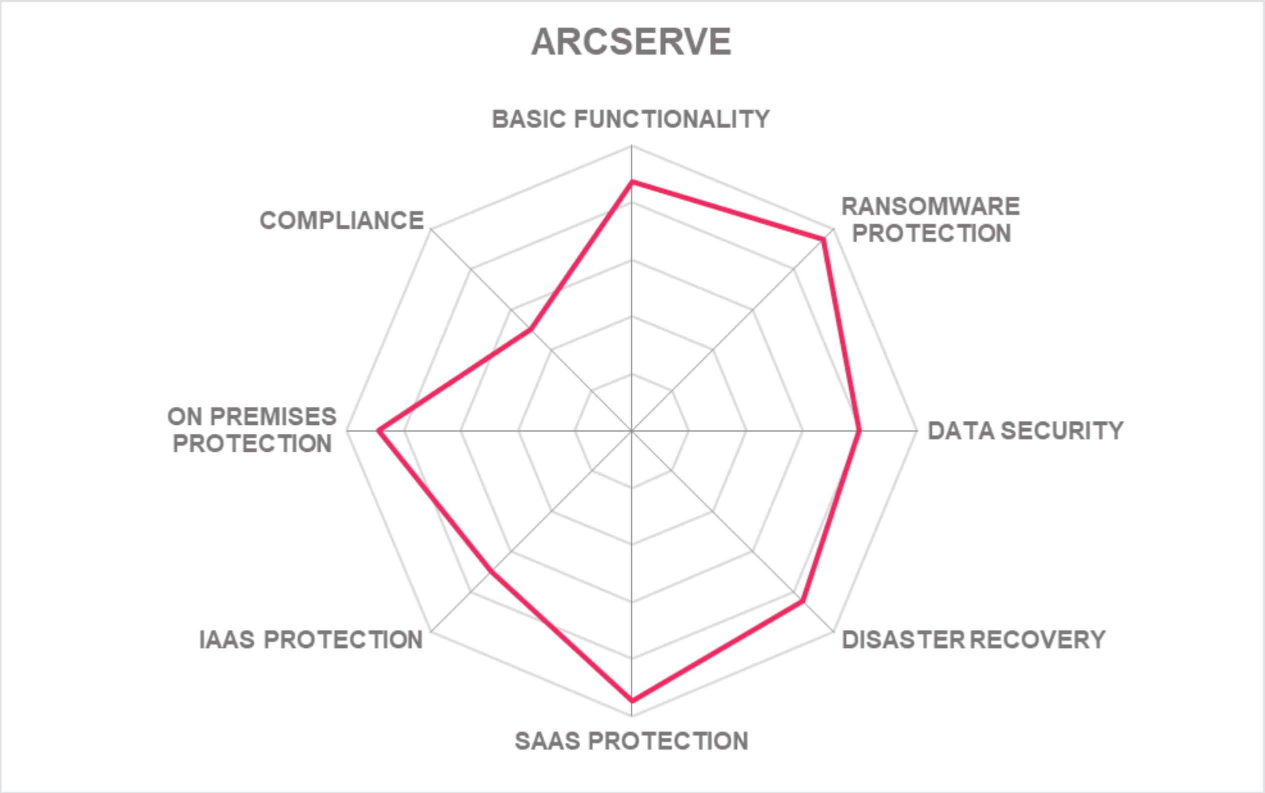
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER



Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors 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 of product features, i.e., a complete assessment.

Types of Leadership

We look at four types of leaders:

- **Product Leaders**: Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders**: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack of global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders**: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders**: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

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
- Deployment
- 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.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree to 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 logical 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.

Vendor rating

We also rate vendors on the following characteristics:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a “good citizen” in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are:

Strong positive
Outstanding support for the subject area, e.g., product functionality, or outstanding position of the company for financial stability.

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral
Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren’t met, while others are well served. For Market Position, it could indicate a regional-only presence.

Weak
Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical
Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don’t appear in a Leadership Compass document due to various reasons:

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- Declined to participate: Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- Lack of information supply: Products of vendors which don’t provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is to provide a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in the Vendors to Watch chapter. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Related Research

Buyers Compass Hybrid Cloud Backup and Disaster Recovery

Market Compass Global IaaS Providers Tenant Security Controls

Leadership Compass: Endpoint Protection Detection & Response

Leadership Brief: Incident Response Management

Leadership Brief: Cyber Hygiene: The Foundation for Cyber Resilience

Leadership Brief: Managing RDP Security Risks to Block Ransomware Attacks

Blog: Hybrid IT Backup and Recovery

Copyright

KuppingerCole Analysts support 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 making 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.