Ovum
TMT intelligence | informa

Ovum Decision Matrix: Selecting a Software-based Data Availability and Protection Solution for the Cloud Era, 2019–20

Publication Date: 10 Dec 2018 | Product code: INT003-000256

Roy Illsley

Summary

Catalyst

According to Ovum's survey data, organizations have approximately 28% of their workloads executing in cloud environments. Much of these cloud workloads is focused on systems of engagement such as websites, office productivity, or collaboration. Ovum's ICT Enterprise Insights Global survey 2017/18 shows that in the next 18 months, organizations will be looking to expand this to more core business workloads such as databases, CRM, and ERP. This shift to a greater proportion of the workloads becoming cloudified, whether migrated to a cloud-native application, moved to a cloud infrastructure, or delivered as a SaaS solution, will require data protection to adapted accordingly. Organizations expect higher levels of system and network availability and cost-effective business continuity in a cloud environment. However, this often leads to the creation of tension between the conflicting demands and priorities of production requirements where access and speed are desired qualities but must also provide resiliency and recovery. The expectation is that data and systems are available as required by the business, so any disruption to this has serious consequences for business operations. This report provides a side-by-side comparison and analysis of leading data protection and availability solutions, looking at the ability to deliver a holistic backup and recovery strategy. The results are delivered as the Ovum Decision Matrix (ODM), which considers the significance of all the core aspects of a backup and recovery strategy.

Ovum view

Ovum research (*ICT Enterprise Insights 2017/18 – Global: ICT Spend and Sourcing*) found the average percentage of the IT management budget spent on data protection is 17%. This level of investment seems high for most organizations, but when Ovum research investigated where the infrastructure investment is being directed, the reason for this spending became clear. The research found that on average, 29.2% of the respondents are planning new or major investments in data protection in the cloud. The combination of the growth in cloud computing with the increased focus on data protection is driven by the lack of trust in this mixed infrastructure environment. Cloud computing and the move to an as-a-service delivery method is also beginning to create tensions and splits in organizations' data protection and availability strategies, with questions being raised about location, security, and latency.

The changing landscape from a world dominated by the VM based on VMware is now beginning to gain momentum as cloud-native technology is more widely adopted. While the cloud-native, or container-based microservices, approach has yet to gain a significant share of the market (it represents only about 2%, according to Ovum's market and survey data), it is expected to increase rapidly over the next couple of years. This shift from a VM-based environment to a more granular container-based environment will create new operational challenges when it comes to data protection.

First, in a container-based environment, the concept of infrastructure as code is becoming more widely understood and adopted by the developer community. The extension of this concept is to extend the "as code" approach to other functionality such as security and data protection. Data

protection vendors do not yet have a strategy for supporting this type of implementation of data protection.

Second, the initial concept of containers is that they are stateless and can be self-healing and controlled by an orchestration layer such as Kubernetes. However, developers have diverged from the original concept and containers can be either stateless or stateful depending on the use case. This makes protecting containerized applications an uncertain task, because it requires some knowledge about if it is a stateful or stateless application.

Finally, containers based on different technologies are being developed. The original containers for x86 are based on Linux, but variants from VMware, Microsoft, and other software companies has created a degree of complexity that has made protecting these workloads more complicated than originally proposed.

The issue for CIOs is that there is an increasing demand to protect the data assets and to make these assets available to a wider audience while not impacting the production operations. To achieve this objective, the different technologies used need to be administered and configured correctly to provide solutions to the many different requirements for resiliency that organizations require. Ovum believes that this management and technology combined represents a powerful combination in enabling organizations to make choices about the type and coverage of data protection and availability needed for their particular circumstances. However, we believe that the thorny issues of budgets, responsibilities, and priorities must be identified and resolved before any strategic data availability plan is implemented. The strategic plan must also take due note of the IT and organizational strategy in terms of the use of new technologies and the readiness to adopt new delivery methods.

Key findings

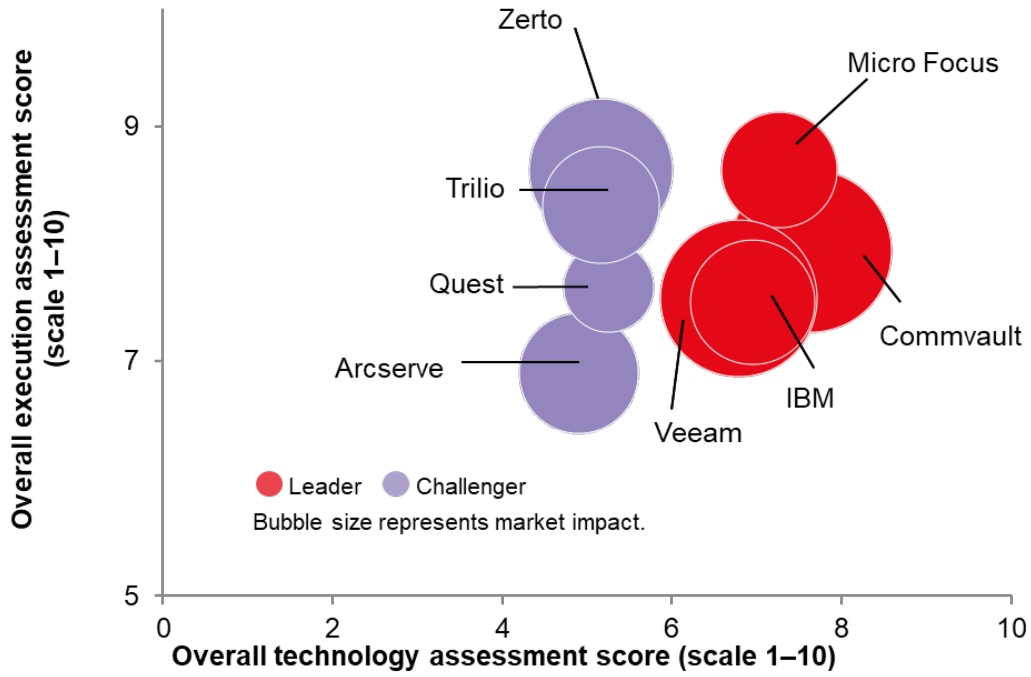
- Commvault is the overall leader and technology dimension leader in the ODM, driven by recent developments and changes to its pricing structure that simplify its deployment and reduce its TCO.
- Veeam is joint second overall in the ODM, but the analysis was based on the software available at the time the report was written and not Veeam's latest release that just missed the cut-off date.
- Micro Focus is the execution dimension leader and joint second overall in its first ODM.
- IBM retains its leadership position for the third ODM in a row with a solid performance across all the dimensions.
- Arcserve, Trilio, Quest, and Zerto are the challengers in this ODM, while a capability gap exists between the leaders and challengers in the technology dimension, the capability is less differentiated in the execution dimension.

Market and solution analysis

Ovum Decision Matrix: Software-based Data Availability and Protection Solution for the Cloud Era, 2019–20

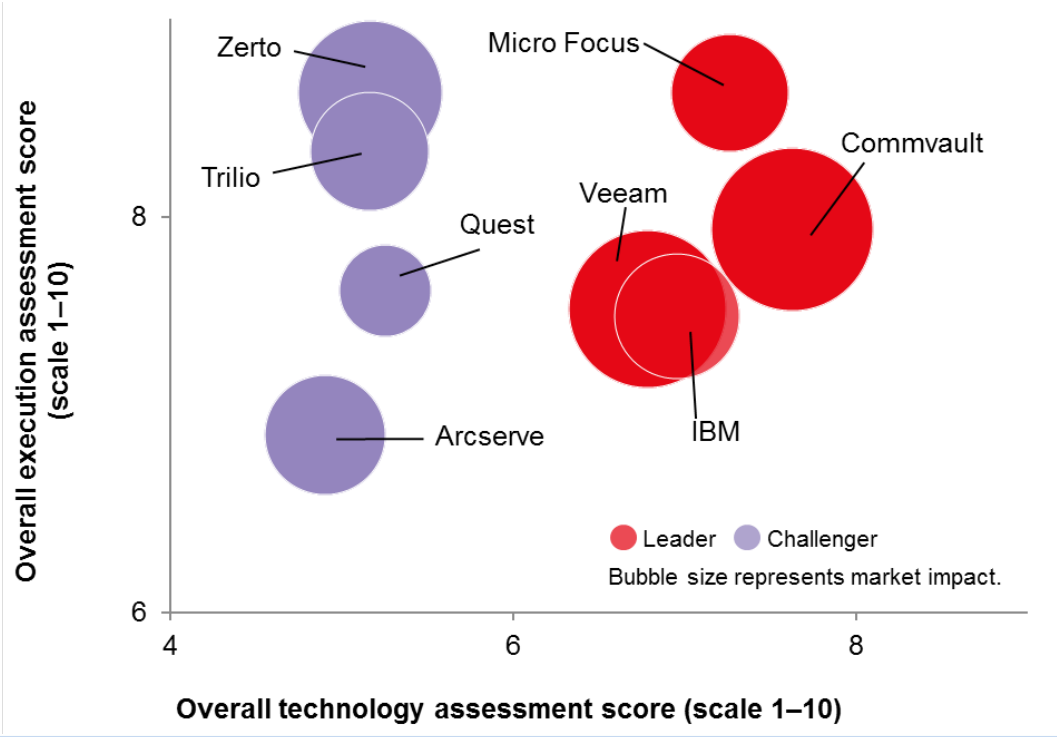
The market in data protection and availability has moved a long way from the traditional backup and recovery approaches that many organizations have used in the past. Today, the cloud has introduced a new layer of capability when it comes to data protection and availability, but technologies such as containers and serverless are creating new challenges. This ODM has evolved over the years and now focuses on how the data assets of an organization can be protected while still providing availability for scenarios such as disaster recovery or accidental data loss. In fact, the term hyper-availability is now being used to describe the business importance of data being available to meet the business demand. The difference from the previous ODMs (2014–15 and 2016–17) is that the longstanding leaders, Commvault, IBM, and Veeam, are now joined by Micro Focus. The interesting feature of this report is that two of the previous leaders (Symantec now Veritas, and EMC now Dell), despite the four-month notice of the production schedule for the report, chose not to participate. Figures 1 and 2 show that even in a mature market there is differentiation between the vendors in terms of technology, while in the execution dimension the difference is less pronounced.

Figure 1: Ovum Decision Matrix: Software-based Data Availability and Protection Solution for the Cloud Era, 2019–20



Source: Ovum

Figure 2: Expanded view of Ovum Decision Matrix: Software-based Data Availability and Protection Solution for the Cloud Era, 2019–20



Source: Ovum

Table 1: Ovum Decision Matrix: Software-based Data Availability and Protection Solution for the Cloud Era, 2019–20

Market leaders	Market challengers	Market followers
Commvault	Arcserve	
IBM	Trilio	
Micro Focus	Quest	
Veeam	Zerto	

Source: Ovum

Market leaders: Commvault, IBM, Micro Focus, Veeam

The leaders in the ODM all demonstrated significant capabilities recording above average scores in nearly all the 19 categories. The leaders were very closely grouped with little to separate them in terms of technology capability, and slightly more in terms of separation in terms of execution capability. Overall, with a normalized score out of 10 across all three dimensions, Commvault was the leader with a normalized average score of 7.60/10 and Veeam and Micro Focus a close second with 7.30/10, with IBM fourth scoring 7.0/10. The degree of difference between the leaders was due to a

few key capability differences in the technology dimension and the consistency in terms of deployment of the solution across all sizes of deployment (SMB, mid-market, and large enterprise).

Market challengers: Arcserve, Trilio, Quest, Zerto

The challengers demonstrated a consistent scoring record being on or just above the average for the different categories. However, within this average score there were significant sub-categories where some of the challengers scored below average, and this was true for at least 25% of the sub-categories. The key differentiator between the challengers and the leaders was seen in the lack of some features, but was most apparent in technology dimension where most of the challengers scored below average for at least two of the sub-categories. This shows that while the challengers have an ability to execute that can match the leaders in at least 75% of the cases, they do not have the wider technology capability yet to be ranked as a leader.

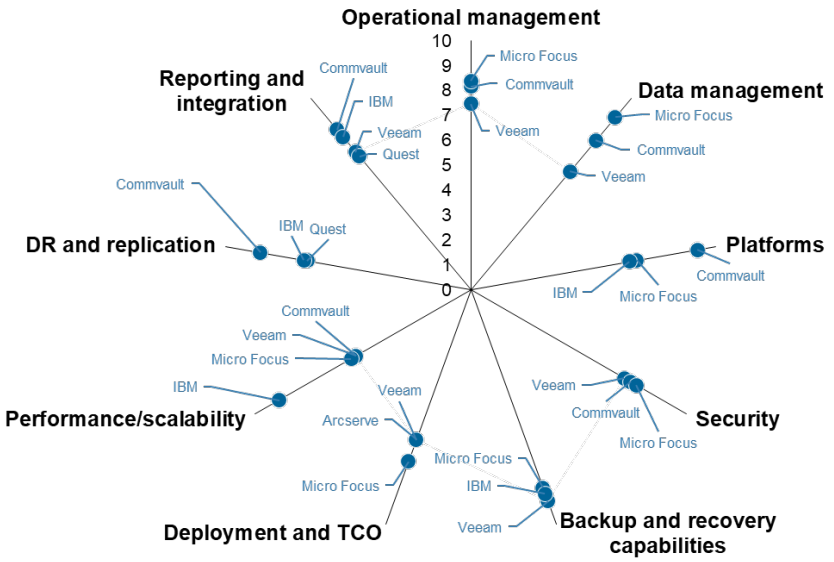
Market followers

Because it is a mature market, none of the vendors in this ODM is classified as a follower.

Market leaders

Market leaders: Technology

Figure 3: Ovum Decision Matrix: Software-based Data Availability and Protection Solution for the Cloud Era, 2019–20: Technology market leaders

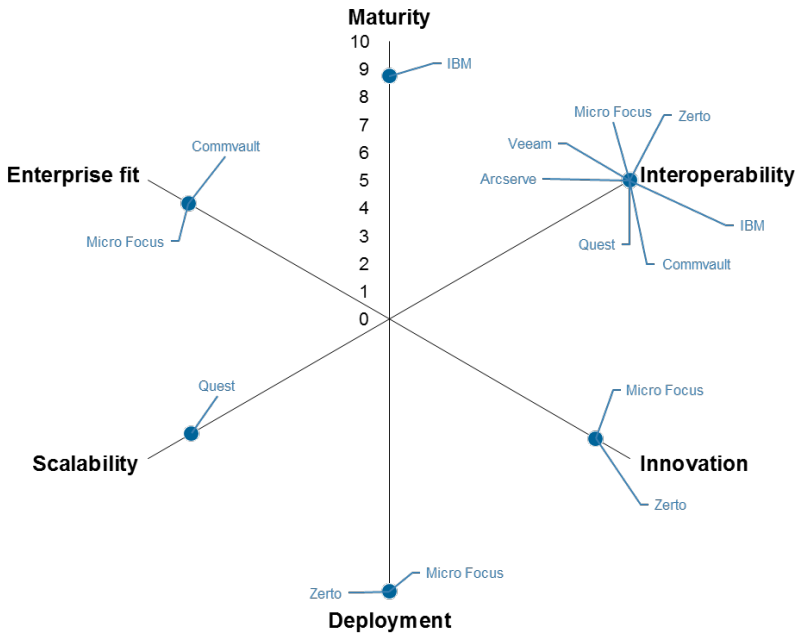


Source: Ovum

Figure 3 shows the top three leaders in the technology dimension by category. Commvault, Micro Focus, and Veeam all appear seven times in the chart, with the other leader, IBM, appearing six times. Quest and Arcserve are the only vendors that are not leaders to appear in the chart. This diagram reinforces the differences between the leaders and the challengers.

Market leaders: Execution

Figure 4: Ovum Decision Matrix: Software-based Data Availability and Protection Solution for the Cloud Era, 2019–20: Execution market leaders

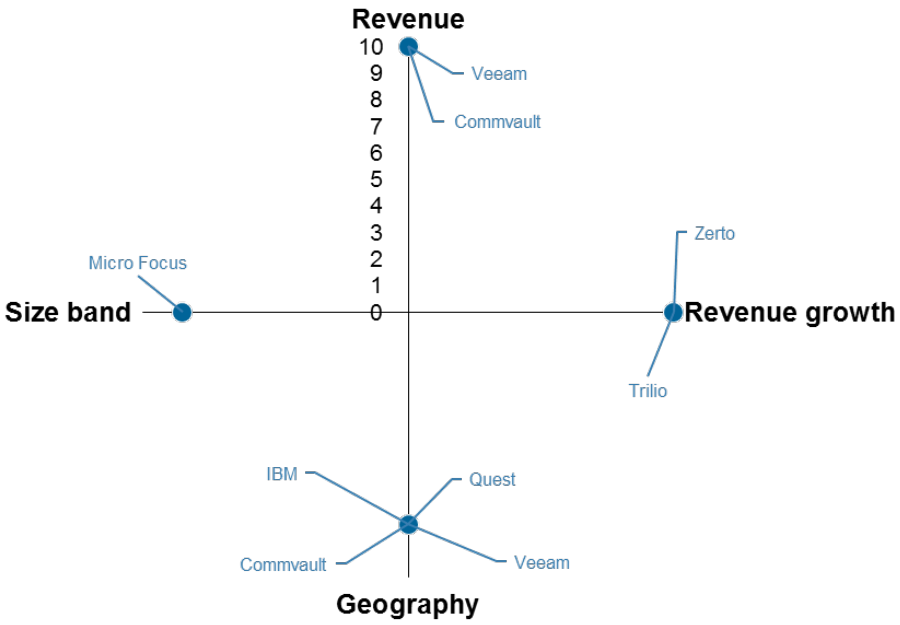


Source: Ovum

In Figure 4 the top scores in the execution dimension are shown by category. Unlike the technology dimension that was dominated by the leaders, the execution dimension is more even. Micro Focus with four appearances is the leading vendor, Zerto is second with three appearances, Commvault, IBM, and Quest recorded two entries, and Arcserve and Veeam complete the list with a single entry each.

Market leaders: Market impact

Figure 5: Ovum Decision Matrix: Software-based Data Availability and Protection Solution for the Cloud Era, 2019–20: Market impact market leaders



Source: Ovum

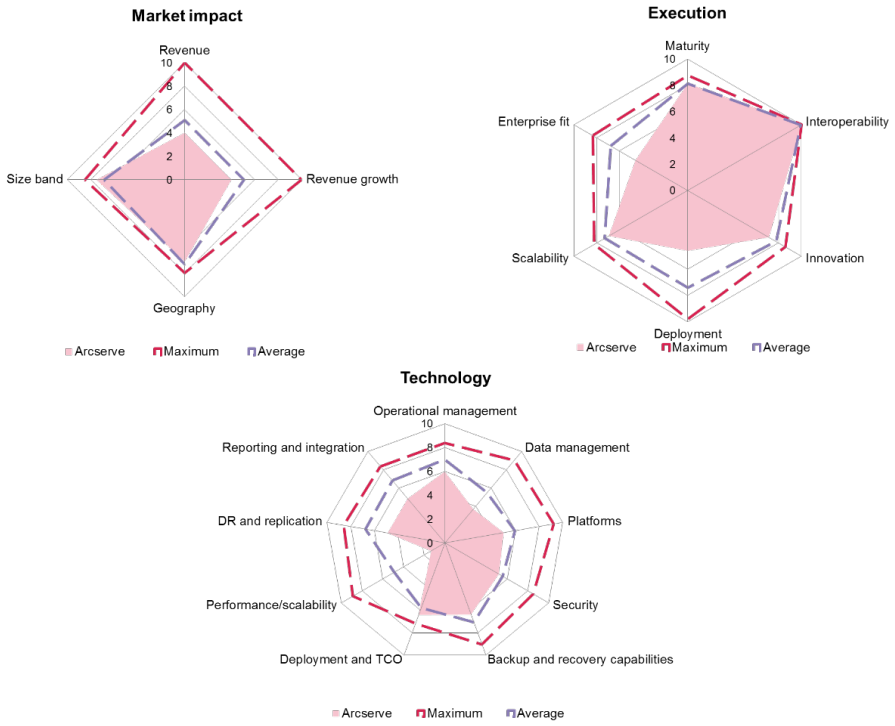
Figure 5 shows the leading vendors in the market impact dimension by category. Commvault and Veeam both recorded two entries, while IBM, Micro Focus, Quest, Trilio, and Zerto all appear once. As expected, Commvault and Veeam are leaders in terms of revenue and geographic coverage, while Trilio and Zerto are the fastest growing but the smallest vendors. Micro Focus demonstrates its broad appeal by leading the size band category.

Vendor analysis

All the scores in the ODM charts and text are normalized to a base of 10, and the allocation of scores was performed according to purely the responses to the questionnaire the vendor completed.

Arcserve (Ovum recommendation: Challenger)

Figure 6: Arcserve radar



Source: Ovum

Products assessed in ODM

Arcserve Unified Data Protection.

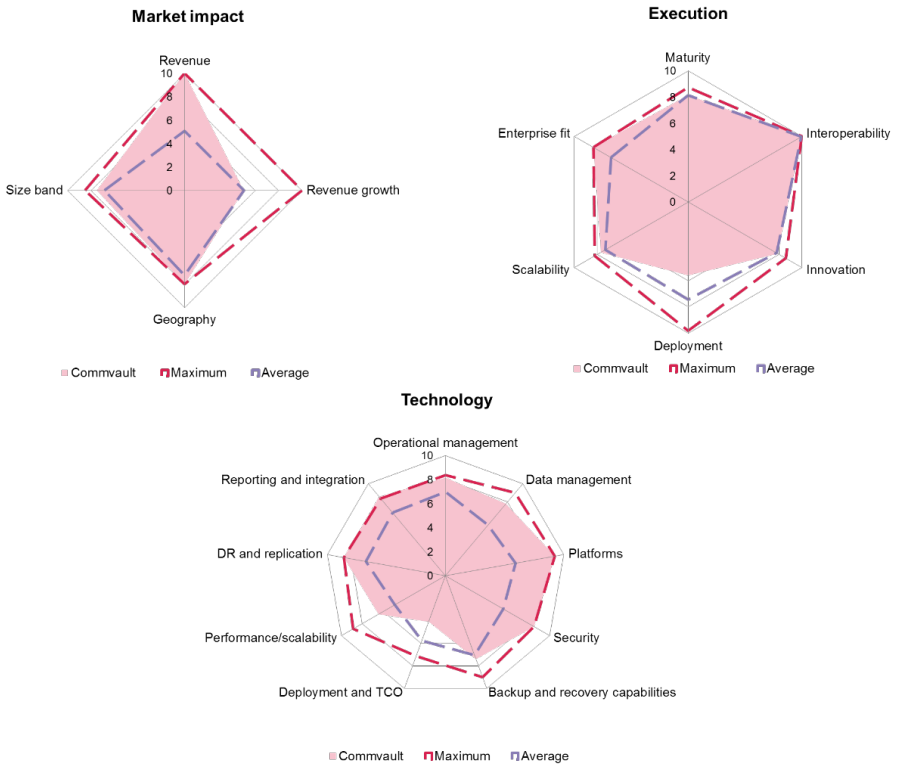
ODM assessment

Arcserve is rated as a challenger despite scoring in-line or above average for all three dimensions. Arcserve scored above average or just below average in over half of the 19 categories and recorded one maximum 10/10 score in the deployment category in the execution dimension. Arcserve was strong in the features (technology) dimension where it recorded all categories above average, but compared to the leaders its scores were not strong enough to change its classification. On average, the final normalized score for Arcserve across all three dimensions was 5.80, which compares to the leaders' average score, which was more than 7.0. However, Arcserve was strongest in the TCO category where it recorded a top-three score and Ovum believes that this is testament to the overall value that Arcserve represents. The deeper analysis of the TCO score finds that Arcserve's ability to back up and recover from media of any age is a significant strength, as is its deployment time of less than 30 minutes, and its software maintenance cost of between 15% and 20%, which makes it one of the most cost-effective vendors. Arcserve's only sub-average score was for the deployment category in the execution dimension. This was something of a surprise given its strength in the TCO section. Arcserve's relative weakness is because of its not having specific market vertical deployment templates, and its deployment time for larger sized deployments being slightly longer than some of its

rivals. Overall, Arcserve provides an above-average performance. It is a solid performer with few stand-out capabilities or significant strengths or weaknesses.

Commvault (Ovum recommendation: Leader)

Figure 7: Commvault radar diagrams



Source: Ovum

Products assessed in ODM

Commvault Complete, Commvault Orchestrate, Commvault Activate

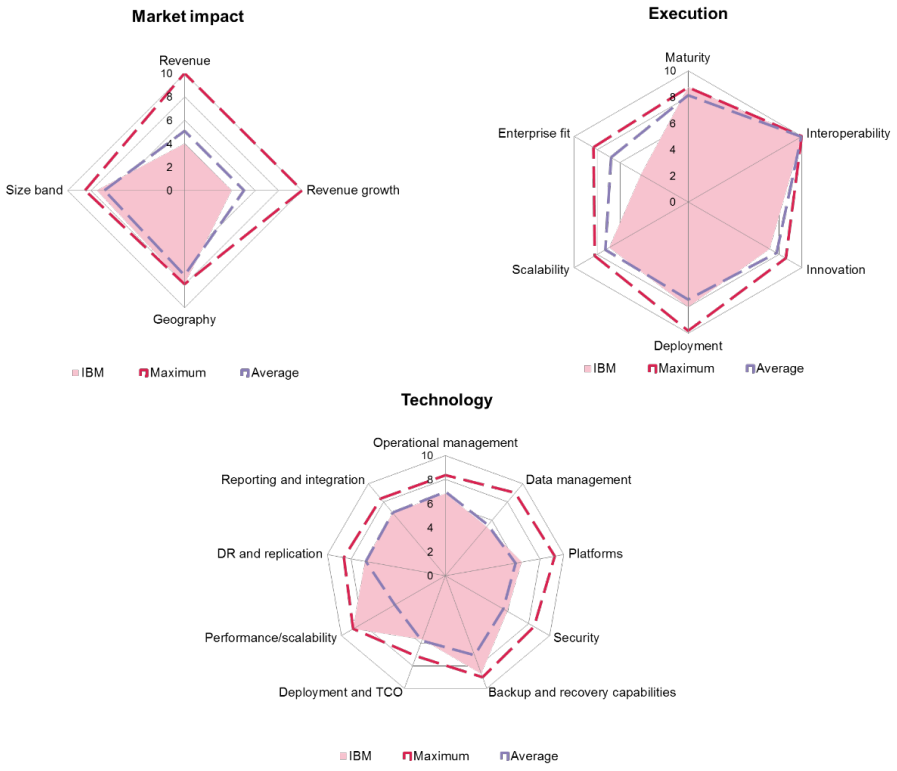
ODM assessment

Commvault remains a leader in the ODM for the second successive time. Commvault's overall average score across all three dimensions was over 7.20, making it the overall leader. Commvault scored above average in all the dimensions, and only two of the 19 categories below average. Commvault's strongest area is the features (technology) dimension where it recorded seven of the nine categories as a top-three score. Commvault's top-three scores in the features dimension were platforms (9.24), DR and replication (8.59), and reporting and integration (8.38). In the platforms category, Commvault's ability to support multiple different operating environments and cloud environments was a key factor in it achieving a near perfect score. However, for Ovum, the most significant capability Commvault displays in the platforms category is its ability to back up and restore container-based environments in terms of both the data lake and container itself. In the DR and replication category, Commvault's ability to replicate data over distances up to 100km and to deliver an RPO in DR mode of between five and 10 minutes is a significant strength. When this is coupled

with the fact that DR mode is not charged for unless it is used makes Commvault Complete live up to its name, a complete solution with no hidden extras. In reporting and integration, the key capability that Commvault delivers is compliance with most of the data privacy and market regulations, which is of significant value to organizations trying to ensure compliance. Overall, Commvault with its new Commvault Complete solution has delivered a backup and replication capability that delivers what the market needs: a simple to use, simple to consume, and cost-effective approach to ensuring data is protected regardless of where it is stored.

IBM (Ovum recommendation: Leader)

Figure 8: IBM radar diagrams



Source: Ovum

Products assessed in ODM

IBM Spectrum

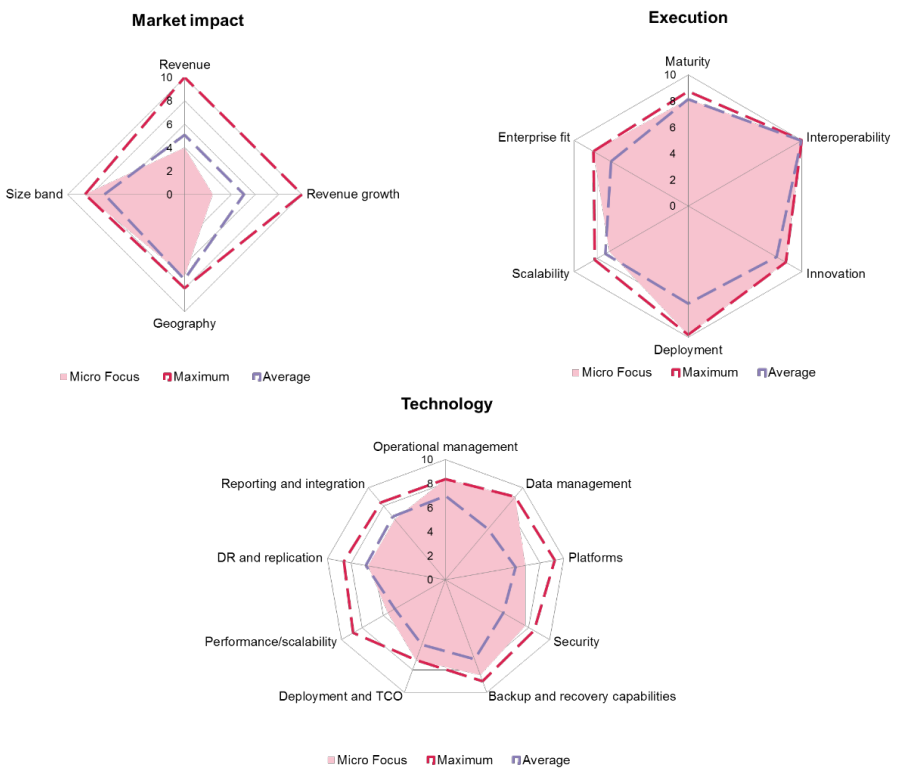
ODM assessment

IBM is classified as a leader in the ODM for the second successive time, and recorded an average score across all three dimensions of 6.78 with an above average score in 16 of the 19 categories across the three dimensions. In the features (technology) dimension, IBM recorded six of the nine categories as a top-three score, with its best performance in backup and recovery (8.71), reporting and integration (8.0), and performance and scalability (10.0). IBM's strength in backup and recovery can be attributed to its multilingual support, with up to 10 languages supported, and its ability to back up a range of environments including VMware vvols and in-memory backup. In reporting and

integration, IBM's strength is its support for the different regulatory environments such as SOX and PCI, plus its level of integration with a number of service desks where tickets can be automatically raised and closed for backup-related incidents. In performance and scalability, IBM demonstrates some significant benefits, including its ability to provide a reference customer with more than 100PB of data being protected, its ability to restore a 200TB file from a 2PB full compressed backup to a cloud location, and assuming a 40Gb/s link in under five minutes using the instant restore capability. Its compression algorithm can reduce both structured and unstructured data to less than 25% of its original size. Overall, IBM demonstrates that it has a market-leading backup and restore solution that meets the needs of the current market. Ovum notes that the IBM solution is not only for large enterprise customers, but also works equally well for mid-market organizations. Mid-market organizations have the same concerns and requirements as large enterprises, it is just they need a solution to be simpler to use and deploy, a capability IBM has developed with its solution as shown by its score in the deployment dimension

Micro Focus (Ovum recommendation: Leader)

Figure 9: Micro Focus radar diagrams



Source: Ovum

Products assessed in ODM

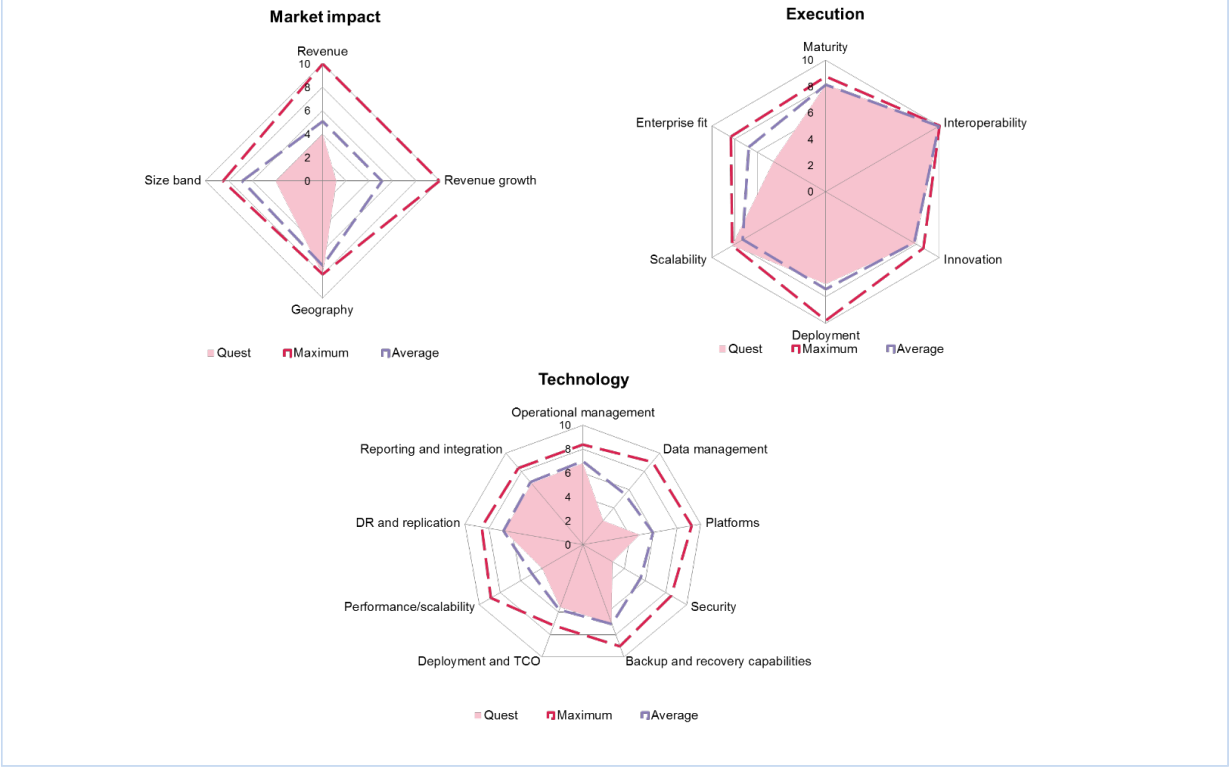
Data Protector

ODM assessment

Micro Focus entered the ODM this year for the first time and is classified as a leader, with an average score across all three dimensions of 6.90. Micro Focus recorded 16 out of the 19 categories in the ODM with a score above the average. In the features (technology) dimension, Micro Focus recorded a top-three score in seven out of the nine categories. Its best performance was in operational management (8.38), data management (9.03), and security (7.67). Micro Focus is particularly strong in terms of its ability to do resource optimization and capacity planning to ensure that backup schedules can be met and SLAs not missed due to resource constraints. Micro Focus is also strong in integrating and supporting snapshot technologies from four different hardware vendors. Data management was Micro Focus's top score and Ovum likes its ability to support with specific optimization a wide variety of data types from audio to video. Micro Focus has also developed a comprehensive application-specific data protection capability. Ovum considers that while customers may not always consider application integrations as they would traditional backup and recovery factors such as workloads etc., the impact of being able to optimize backup for data types and applications provides the administrator with a degree of flexibility so that differing SLAs can be applied if needed. Ovum believes that the company's approach to data policies enables it to ensure that data can be restored to only the locations/people that it is supposed to be available in/to. Micro Focus also demonstrates a good awareness of the risks of ransomware and provides malware protection. Overall, Micro Focus has a very good solution that delivers a well above average performance, with some category-leading capabilities.

Quest (Ovum recommendation: Challenger)

Figure 10: Quest radar diagrams



Source: Ovum

Products assessed in ODM

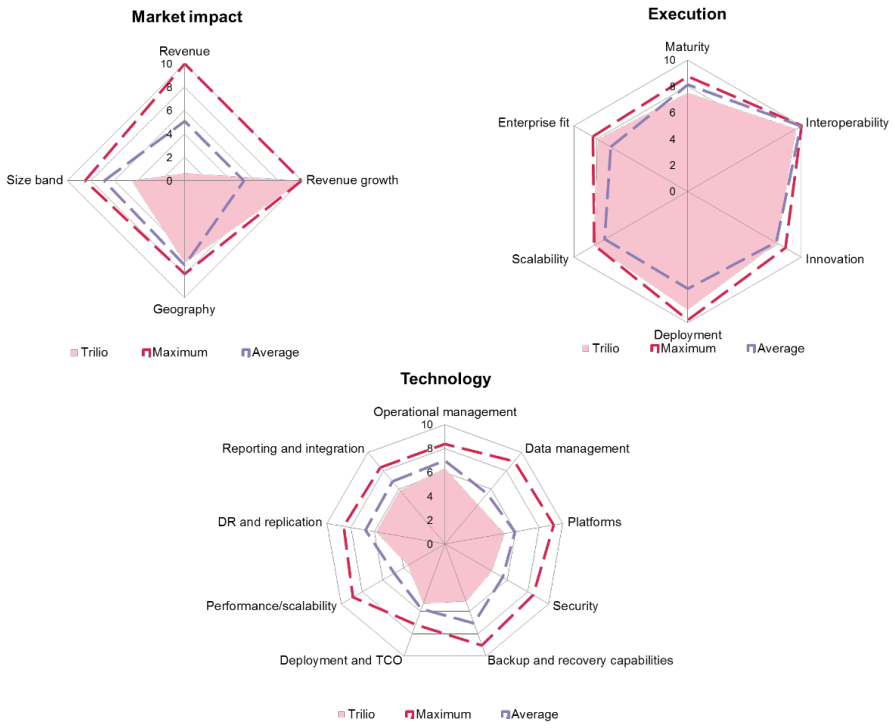
Rapid Recovery version 6, and NetVault version 11.

ODM assessment

Quest is in the ODM for the second time. The first time it was under the Dell umbrella, but this time it has entered as an independent vendor. Quest is classified as a challenger, with an average score across all three dimensions of 5.70, and above average or just below average scores in 12 out of 19 categories. Quest is strongest in the execution dimension, where it recorded a maximum 10.0 for interoperability. Quest also recorded three top-three scores in the features (technology) dimension and is particularly strong in reporting and integration (6.97) and operational management (6.82). Ovum believes that Quest's strength in reporting and integration is due to its support for all the different regulatory compliance frameworks, and its ability to provide best-practice reporting across a number of different scenarios. In operational management, Quest's strength is its ability to work natively with at least three different storage vendors. Overall, Quest performed well but was let down by a lack of capability in a couple of areas: data management and security, where it either did not have the capability or relied on third-party solutions.

Trilio (Ovum recommendation: Challenger)

Figure 11: Trilio radar diagrams



Source: Ovum

Products assessed in ODM

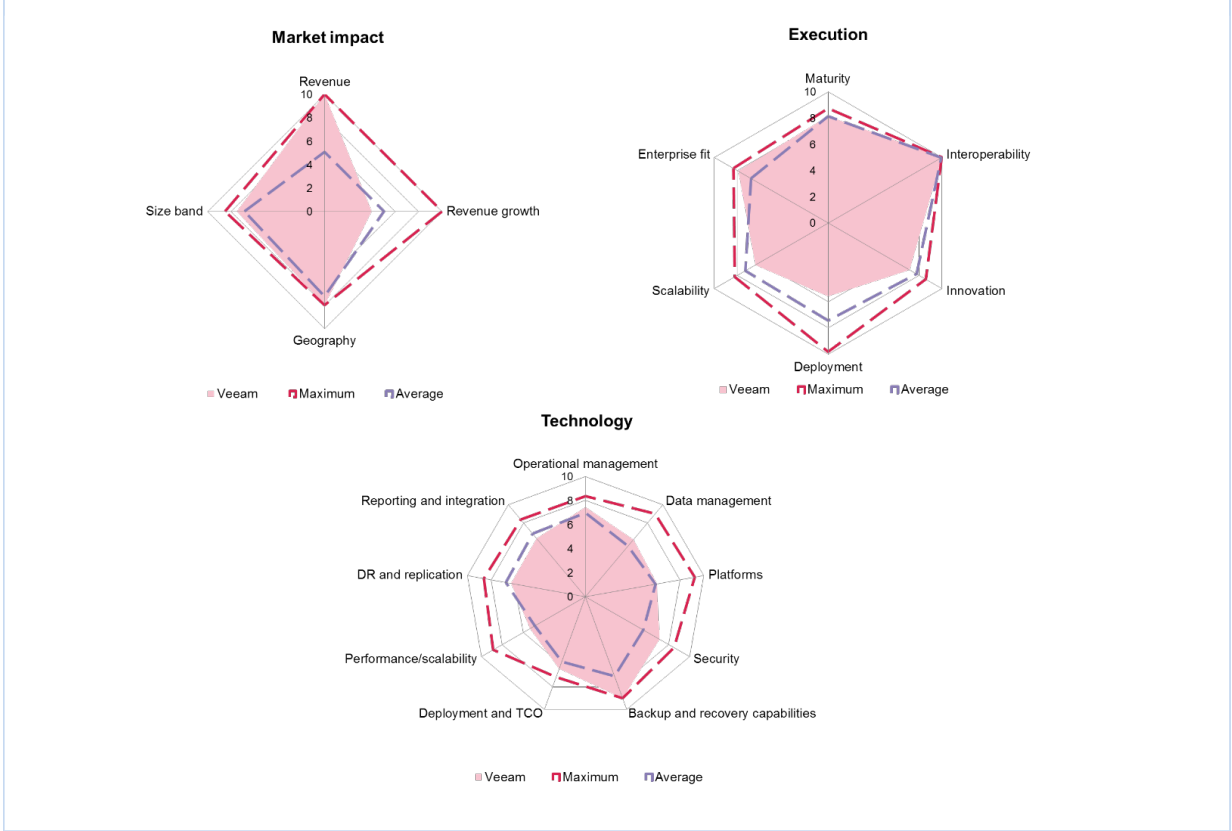
TrilioVault

ODM assessment

Trilio in its first ODM is classified as a challenger, with an average score across all three dimensions of 6.19, which was the closest challenger to the leader group in terms of overall score. Trilio was just below or above average in 11 of the 19 categories, with its size contributing to one below-average score: revenue in the market impact category. While Trilio in the features (technology) dimension did not record any top-three scores, it did come fourth on a number of occasions. Trilio scored well in terms of execution, and was one of the top vendors with an average score of 7.98 thanks mainly to it being one of the most cost-effective vendors in the ODM. Ovum believes that the financial investment needed to implement Trilio in all the different scenarios in the ODM demonstrates it value, and when this is combined with the fact Trilio is also one of quickest solutions to deploy across all the scenarios, it becomes even more cost-effective. Overall, as a new entrant in the data protection market, Trilio has a good solution. Its score was affected by its small size and relative immaturity, but it scored well for innovation and growth. Ovum believes that Trilio is a potential market leader in a future ODM because its core capability is focused on cloud-native technologies and not just legacy VMs.

Veeam (Ovum recommendation: Leader)

Figure 12: Veeam radar diagrams



Source: Ovum

Products assessed in ODM

Veeam Hyper-Availability Platform

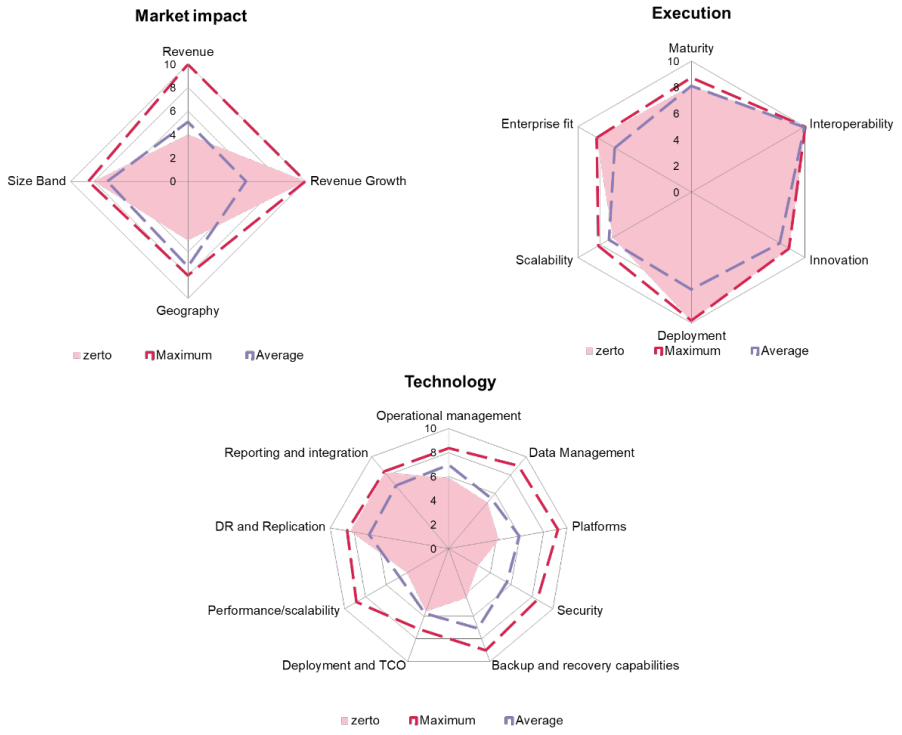
ODM assessment

For the second successive ODM, Veeam is classified as a leader and recorded above average or just below average scores in 16 of the 19 categories. Veeam's performance was consistent with backup and recovery, deployment and TCO, and security its strongest three categories in the technology dimension. In terms of backup and recovery, Veeam is the leader for this category, a key differentiator is that it can globally restore a common file that may be on multiple individual devices and shared devices to a single version. As data volumes grow and organizations deal with multiple copies of the same data, the ability to simplify and restore data to a single version becomes an important consideration in reducing complexity for users. In deployment and TCO, Veeam's strength is its ability to restore from media of any age, which for organizations that are more than five years old is a reality they live with. Organizations have so much data stored on media that dates back many years, and from time to time this needs to be recovered and incurs an additional expense, hence its part in making Veeam a good TCO solution. Veeam's final key strength in terms of technology is security. Security from a backup and protection aspect is a vital capability. Veeam's performance in terms of security is above average because it provides full data encryption, the ability to set policies for data based on location, and its ability to provide a secure way to recover from a ransomware attack.

Veeam is one of the biggest vendors in the software data protection and availability sector and is growing at one of the fastest rates of all the vendors in this ODM. In terms of execution, Veeam is also above average in terms of interoperability where it recorded a maximum 10/10, and is also a clear leader in terms of enterprise fit. Veeam's other strength is its maturity in the market and its ability to listen to its customers and deliver the solutions they need when they need them.

Zerto (Ovum recommendation: Challenger)

Figure 13: Zerto radar diagrams



Source: Ovum

Products assessed in ODM

IT Resilience Platform

ODM assessment

Zerto is classified as a challenger in the ODM. The classification is based on its nine well-below-average category scores across all 19 categories, which when compared to the leader, which recorded zero below-average categories, impacted its overall normalized score of 5.40. Zerto was strongest in the execution dimension, where its speed to deploy and cost advantage is a clear area where Zerto is above average. Zerto is also strong in terms of reporting and integration in the technology dimension, with a score of over 6.50. Ovum found its ability to provide detailed performance and resource utilization reporting provided good insight into the value and service that organizations are obtaining from its data assets. Overall, Zerto's performance was good, with a few areas of weakness due to its product not being developed to deliver capabilities, which is not an issue except the rest of the market has expanded to include capabilities such as security and data management. Ovum would expect Zerto to increase its breadth of coverage by forming partnerships with vendors with these complementary solutions.

Emerging vendors

Table 2: Emerging vendors: Software-based Data Availability and Protection Solution for the Cloud Era, 2019–20

Vendor	Product
Citrix	Citrix Workspace and Citrix Analytics
Continuity Software	AvailabilityGuard
iland	iland Disaster Recovery-as-a-service
Imanis Data	Imanis Data Platform

Source: Ovum

Citrix

Providing data protection does not just mean backing up data and being able to restore it, even though most vendors in the market are focused on this approach. When talking to CISOs, risk management and increasing trust are the key responsibilities of the CISO. Workspace and analytics drive these two principles, focusing on outcomes and protecting the future of work. Citrix provides two alternative approaches that complement the backup market in data protection by taking a more holistic view. First, Citrix provides a suite of products that allow for applications and data to be delivered securely to end users. Second, it uses advanced analytics to enable users to understand the behaviors of the data and to assess the risk and threat level that a situation presents. While many would not see these as part of the data protection plan for the organization, Ovum believes that these aspects are required to ensure that any backup data is not compromised and can therefore be trusted as the source of recovery.

Citrix Workspace

One of the first challenges in data protection is to ensure that users' data and applications can be recovered and made available so that business operations can continue. It just as important, however, to avoid data loss and security breaches. Citrix Workspace provides a solution to not only manage the applications and data, but also to secure and protect them. Citrix Workspace operates across a wide range of different application types, from SaaS to on-premises, and aggregates all the applications and data so that it is delivered and managed in a single, unified way. In January 2017, Citrix acquired Unidesk, which developed the original application layering solution. This technology captures every component of a Windows workspace (OS, applications, and user data) as independent virtual disks. These are then delivered as a personal workspace by stacking layers in any order through simple point-and-click assignment and Active Directory entitlements.

Citrix Analytics

The ability to ensure file integrity and protection of intellectual property requires organizations to adopt a different approach to trust relationships. Understanding the behavior of data and users is a critical element of being able to provide data protection and demonstrate this trust to organizations. With its

Analytics solution, Citrix gathers data on the environment and behavior of the users and data, and by using AI and machine learning technologies, it can establish any behavior that is suspicious or anomalous. Understanding the data at this level enables organizations to identify areas that represent a risk to the organization. Ovum believes that as part of any data protection plan, visibility into the data and behaviors are key aspects of being able to ensure that the backups are executed correctly and the data is secured. The added bonus with Citrix Analytics is that it helps organizations to understand the security and performance aspects that can be used to modify the environment.

Continuity Software

Continuity Software has developed a specific risk mitigation solution to ensure that systems and services are always available. Today, the IT environment that needs to be guaranteed to deliver the critical services that organizations need is distributed over a wide range of different platforms. Continuity Software has developed a management layer solution that spans these environments to provide the ability to identify, remediate, and prevent outages. AvailabilityGuard is designed to identify any configuration drift, misconfiguration, or deviation from industry best practices. AvailabilityGuard's approach uses a simple four-stage process: scan, correlate, detect risk, and improve.

Scan

The first stage of the process is to gather all the information on the environment. AvailabilityGuard uses an agentless approach and makes use of existing data sources such as CMDBs. The scan phase is an event-driven scheduled background operation that looks across the entire environment for known vulnerabilities or misconfigurations (compared to a set of standard configuration templates). This scan covers all aspects of the environment including servers, storage, databases, virtualization, and the cloud.

Correlate

The scan identifies and detects the different elements in the environment, but this is just the data-gathering phase of the process. The correlate phase performs the matching of the information to the assets and to the defined, known "good state". The correlation phase takes into consideration both the technical as well as business levels of any known good state. The variations between the current state and the defined state are produced in the form of topology maps that clearly show IT staff where to focus their attention.

Detect risk

The correlated data is compared to a database of more than 7,000 vendor-issued best practices as well as locally developed policies. The outputs from this detection phase is automatically generated and ranked so that the high-risk critical issues are clearly identified. This automated risk assessment and ranking is particularly useful to IT operational teams because it enables them to focus their efforts on the most important issues. The other key aspect of AvailabilityGuard is that it overlays the business view of these services, so the ranked report ensures the business priority is considered.

Improve

The improve phase takes the management of complex environments to the next level, with many IT departments focused on firefighting and ensuring that service availability is restored quickly. Improve provides the analysis of the environment so that potential disruption can be avoided and the entire

environment can be seen through different lenses, such as data safety and system availability. Ovum particularly likes that AvailabilityGuard in this phase provides actionable information to help organization improve.

iland

The value proposition of iland's DRaaS is based on four key principles: security, exceptional support, availability, and integrated management. Ovum believes that for most organizations, DR is seen as an expensive insurance policy that they have little confidence in should they need it. Iland's DRaaS solution combines these four principles but is also cost-effective, helping organizations reduce the overhead costs associated with setting up and managing any DR plan.

Security

The general concern of many CIOs is that the cloud is inherently less secure than an on-premises solution. *ICT Enterprise Insights 2017/18 – Global: ICT Drivers and Technology Priorities* discovered that 55% of respondents put managing security as one of their top-three challenges for 2018. Iland includes in its DRaaS offering an impressive array of security features. These include vulnerability scanning, encryption, antivirus and anti-malware protection as part of the service, which is fully managed by iland's security team. A comprehensive monitoring capability covers not only the integrity of the data, but also extends to cover web reputation monitoring and cover to block any denial of service attacks.

Support

A central capability for most organizations adopting cloud services is the availability of 24x7 regional support, and the professional services that can help them with the adoption of cloud. Iland has developed a support infrastructure and a team of architects that help organizations to smooth the adoption of these services and ensure they get the best value from any investment in cloud computing. For DRaaS, this support extends to helping with DR failover and failback when required as well as with the setup and management of virtual protection groups.

Availability

The concept that any disaster can be mitigated by a backup site within the metropolitan area was somewhat disrupted in 2005 by Hurricane Katrina in the US, where primary and secondary data centers were both destroyed over a 100km area. Even more than the threat of natural disasters are the threats that hacking, viruses, ransomware, and even human error can pose to companies. Iland has a global set of eight data centers that provide primary and secondary DR locations for its customers. These data centers are all tier-3-rated, and many have tier-4 capabilities such as guaranteeing 99.982% availability, but due to location cannot be classified as tier-4.

Integrated management

The ability to manage the DR solution and to test and execute a failover is one of the capabilities that many solutions fail to make as simple as CIOs would like. Much of the cost of DR is in the management, setup, and ongoing maintenance. With iland's DRaaS service, these costs are removed and replaced with a simple pricing model encompassing a per-VM fee, a storage and bandwidth fee, and the cost of any running VMs (such as a domain controller). The integrated management console is an example of how iland is reducing the management overhead for organizations. From this

console, failover and failover testing can be performed, and the built-in compliance testing and reporting provides organizations with an auditable report confirming the DR coverage and its level of compliance to any regulations under which the company operates.

Imanis Data

Imanis Data is a data protection solution for Hadoop and NoSQL environments. The challenge with Hadoop and NoSQL is that the architecture of the solution is based on distributed data, but this architecture does not provide complete data protection. In fact, this distributed approach complicates the task of providing data protection, and is typically not addressed by the traditional data protection vendors. The big problem with the distributed architectures is that any corruption could be propagated throughout the entire deployment. Organizations therefore require a data protection solution designed to deal with the unique challenges and benefits that big data solutions present.

Imanis Data Platform

The Imanis Data Platform (IDP) is based on three simple value propositions: the ability to scale, being data-aware, and making use of AI and machine learning.

Scale

To match the architecture of big data solutions, the IDP software uses commodity hardware. Each node in the IDP uses directly attached storage to the server node so that expensive NAS and SAN technology is not required. The key principle of IDP is that each node in the data cluster is connected to more than a single node, creating a mesh effect so that data transfer can be parallelized. IDP can be installed on bare metal or VMs, and supports the most popular Linux distributions: RHEL, Ubuntu, Oracle Linux, and Centos. The complexity of big data environments and the movement of data within them makes using an agent-based approach to management inefficient. IDP therefore uses the native interfaces of the big data platforms as its cross-system communication pipeline. Another aspect of scale that IDP addresses is that of backup strategy. Imanis Data employs an incremental-only backup strategy, which is more relevant for big data technologies. The software ascertains what has changed since the previous incremental backup, and then backs up only that information. This incremental data is immediately materialized onto Imanis Data servers, and a restore point is created to enable single-step data recovery.

Data awareness

One of the big differences with data protection of big data to other data protection environments is the need to understand not only the data, but also the schema the data is part of. One of the challenges with backup and restoring data in big data environments is the ever-changing topology of the data. IDP does not attempt to preserve the source and target topology. It dynamically acquires the topology of the destination cluster at the time of the restore. It then uses this structure to restore the backed-up data to match the topology of its destination. IDP also includes a data-masking capability so that any data can be made available to application testing teams. Imanis Data has a patent-pending, one-way masking algorithm that protects the sensitive information and ensures that it cannot be exploited for unscrupulous purposes.

Machine learning

IDP uses machine learning technology so that it can understand the context of the data and deliver the optimum data protection for each environment. The capabilities of Imanis Data machine learning are focused on three aspects;

- Optimizing the backup performance and timing by understanding the business imperatives in terms of restore point objectives and restore time objectives.
- Detecting and mitigating security threats including ransomware.
- Optimizing storage utilization for the best performance.

Vendor solution selection

Inclusion criteria

The software-based data availability and protection market has many vendors that offer solutions to customers of all sizes. However, the criteria to be included in this Ovum Decision Matrix are based on the ability to offer solutions for a range of enterprise customers of different sizes and with a different mix of technologies, even though x86 is the dominant technology in use and therefore any solution must operate in the x86 market. It must be noted that Dell EMC, ExaGrid, and Rubik declined to take part in this edition of the Ovum Decision Matrix.

The criteria for inclusion of a vendor in this *Ovum Decision Matrix for Software-based Data Availability and Protection in the Cloud Era 2019 – 20* are as follows:

- The vendor must be a global vendor and have customers in at least two of the three regions: Asia-Pacific, EMEA, and North America.
- The vendor must offer data availability and protection capabilities that enable management of data across all different types of media and must include at least two of the following: spinning disk, tape, cloud, or flash storage.
- The vendor must have at least 500 customers, and these must comprise a mix of midsize and large enterprises.
- The vendor solution must have at least one reference customer with more than 200TB of data under management using its solutions.

Exclusion criteria

The data availability and protection market is considered a separate but closely associated category of the backup and recovery market. Ovum accepts that for some vendors, this is how they have entered this market, but this is not universally the case, and the solutions being evaluated are those specifically sold to enterprise customers. Vendors and products excluded from the analysis are determined on the following criteria:

- The vendor‘s solution is only applicable to five of nine different classifications in the features matrix (operational management, data management, platforms, security, backup and recovery, reporting and integration, deployment and TCO, performance and scalability, and DR and replication).

- The vendor's solution is more than 50% made up of partner solutions or third-party solutions.
- The vendor has no direct contact with end customers, with everything done through channel partners. Ovum accepts that some vendors have a channel sales-only approach, but these customers must have some process for direct customer interaction should the customer request it.

Methodology

Technology assessment

Vendors were invited to complete a data availability and protection features matrix, a comprehensive spreadsheet listing the product features that Ovum believes are required and desirable in a data availability and protection solution. The features matrix is a comprehensive technology questionnaire developed by Ovum analysts, containing hundreds of different criteria. Ovum then applied weights to these entries by individual row and section, based on the importance of each criterion. The final ranking of vendors in the technology dimension is based on the scores vendors achieve from this analysis.

The criterion for a vendor to answer "yes" to a feature is that it must be available out-of-the-box in any product within its range of products that are applicable to its data availability and protection solution. A third-party provider, custom integration, or partnership is not sufficient to merit a "yes". All vendors were made aware of this prior to completion of the questionnaire, and before publication of the report, vendors were given the opportunity to review their submissions again to ensure there were no discrepancies.

In this assessment dimension, Ovum analysts developed a series of features and functionality that provide differentiation between the leading solutions in the marketplace. The criteria groups identified for technology/service area are as follows:

- Operational management: One of the key aspects of any management tool is how well it fits into existing processes and operational procedures, and whether the solution imposes any significant operational management overheads.
- Data management: At the core of any data availability and protection solution is its ability to understand and manage the data.
- Platforms: The breadth of coverage that a solution supports is an important feature in terms of the potential audience and how well the solution fits with an organization's architecture.
- Security: This capability looks at the ability of the solution to deliver different levels of security to match those needed by the different classification of data.
- Backup and recovery capabilities: This capability considers the process of backing up data and the recovery of data. It looks at how the solution supports the many different management requirements, types, scheduling, and so on of these backups.
- Reporting and integration capabilities: The ability to derive some metrics and understanding of the cost and value of the service as well as the ease of integrating with adjacent technologies.
- Deployment and TCO: Referring to a combination of assessed criteria and points of information, Ovum analysts provide detail on various deployment and TCO issues, including time, services, and support.

- Performance and scalability: Points of information are provided to show the scalability of the solution across different scenarios and the general performance capability.
- DR and Replication: Replication extends the scope of the solution to cover both HA/CA and BC/DR use cases.

Execution

In this dimension, Ovum analysts review the capability of the solution around the following key areas:

- Maturity: The stage that the product/service is currently at in the maturity lifecycle, relating to the maturity of the overall technology/service area.
- Interoperability: How easily the solution/service can be integrated into the organization's operations, relative to the demand for integration for the project.
- Innovation: Innovation can be a key differentiator in the value that an enterprise achieves from a software or services implementation.
- Deployment: Referring to a combination of assessed criteria and points of information, Ovum analysts provide detail on various deployment issues, including time, industries, services, and support.
- Scalability: Points of information are provided to show the scalability of the solution across different scenarios.
- Enterprise fit: The alignment of the solution and the potential ROI period identified.

Market impact

The global market impact of a solution is assessed in this dimension. Market Impact is measured across four categories, each of which has a maximum score of 10.

- Revenues: Each solution's global backup and recovery solutions revenues are calculated as a percentage of those of the market leader. This percentage is then multiplied by a market maturity value and rounded to the nearest integer. Overall global revenue carries the highest weighting in the market impact dimension.
- Revenue growth: Each solution's revenue growth estimate for the next 12 months is calculated as a percentage of the growth rate of the fastest-growing solution in the market. The percentage is then multiplied by 10 and rounded to the nearest integer.
- Geographical penetration: Ovum determines each solution's revenues in three regions: the Americas; Europe, the Middle East, and Africa (EMEA); and Asia-Pacific. These revenues are calculated as a percentage of the market leading solution's revenues in each region, multiplied by 10, then rounded to the nearest integer. The solution's overall geographical reach score is the average of these three values.
- Size-band coverage: Ovum determines each solution's revenues in three company size bands: large enterprises (more than 5,000 employees), medium-sized enterprises (between 1,000 and 4,999 employees), and small enterprises (fewer than 1,000 employees). These revenues are calculated as a percentage of the revenues of the market leader in each region, multiplied by 10, and then rounded to the nearest integer. The vendor's overall company size-band score is the average of these three values.

Ovum ratings

- **Market leader:** This category represents the leading solutions that we believe are worthy of a place on most technology selection shortlists. The vendor has established a commanding market position with a product that is widely accepted as best of breed.
- **Market challenger:** The solutions in this category have a good market positioning and are selling and marketing the product well. The products offer competitive functionality and good price-performance proposition, and should be considered as part of the technology selection.
- **Market follower:** Solutions in this category are typically aimed at meeting the requirements of a particular kind of customer. As a tier-one offering, they should be explored as part of the technology selection.

Ovum Decision Matrix Interactive

To access the data availability and protection Ovum Decision Matrix Interactive, an online interactive tool providing you with the technology features that Ovum believes are crucial differentiators for leading solutions in this area, please see the *Ovum Decision Matrix Interactive* tool on the Ovum Knowledge Center.

Appendix

Methodology

- Detailed technical briefings were conducted with each vendor in the report.
- A detailed spreadsheet of capabilities was completed by the vendor and reviewed by the analyst and peer reviewed to ensure accuracy.
- Supplemental information was obtained from vendor literature and websites, other Ovum surveys, and Ovum's data products/market forecasts.
- The article was peer-reviewed by at least two different analysts/consultants.

Author

Roy Illsley, Distinguished Analyst, Infrastructure Solutions

roy.illsley@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com

askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing

Boston

Chicago

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

Paris

San Francisco

Sao Paulo

Shanghai

Singapore

Sydney

Tokyo