Ovum
TMT intelligence | informa

Ovum Decision Matrix: Selecting a Data Availability and Protection Solution for the Cloud Era, 2016-17

Summary

Catalyst

Organizations are demanding higher levels of system and network availability, and cost-effective business continuity. However, all this must be managed and maintained by a single department with one IT budget. This often leads to the creation of tensions between the conflicting demands and priorities of production requirements where access and speed are desired qualities but must also provide resiliency and recovery. The main area of contention is the distinction between business continuity (BC), disaster recovery (DR), backup and recovery, and the role of cloud-based solutions. The question for many is how these different approaches share the budget to deliver what the end user wants, and how to minimize the impact of any loss of data or service. This report provides a side-by-side comparison 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 three aspects of a backup and recovery strategy and how these influence how technology is deployed, used, and controlled.

Ovum view

Backup and recovery are aspects of systems management that are typically forgotten about until they are needed. However, managing the production systems and the backup systems as a single entity has significant benefits as well as significant challenges. Technology advances have created the position where providing the infrastructure to provide resiliency does not have to mean redundant and expensive capacity, and the systems can be used as part of an active backup plan. However, security remains a key issue with all aspects of data protection, and Ovum believes that this area represents the next wave of product innovations.

The terminology surrounding the concept of data availability is creating market confusion. For example, continuous availability (CA), high availability (HA), fault tolerant (FT), BC, and DR have been used by the x86 virtualization vendors because potential data availability provides benefits from using the virtualization technology. Cloud computing has introduced many more products on the market offering solutions that address the issues surrounding the question of how to provide a differentiated level of service availability based on business priority. The solutions nearly all operate across both the on-premise (physical and virtual environments) as well as the different flavors of cloud environments.

Ovum research (ICT Enterprise Insights 2015/16 – Global: ICT Spend and Sourcing, n=1,580) found the average percentage of the IT management budget spent on data protection was 16%. This level of investment seemed high for most organizations, but when Ovum research investigated where the infrastructure investment was being directed, the reason for this spending became clear. Ovum research (ICT Enterprise Insights 2015/16 – Global: ICT Drivers and Technology Priorities, n=4,750) found that on average, 40% of the respondents were planning new or major investments in IaaS based on public clouds, compared to 43% of respondents investing in private on-premise clouds. 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 issue for CIOs is that these technologies need to be administered and configured correctly to provide solutions to the many different requirements for resiliency that organizations demand. Ovum

believes that the management and technology combined represent 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 readiness to adopt new delivery methods.

Key findings

- Veeam improved its position from the previous ODM 2014-15 and is now the clear market leader, demonstrating a consistent above average performance with five sub-category leading scores as well as being the leader in the market impact category and features categories.
- IBM remains in the leadership classification, and is the leading vendor in terms of the number of sub-category leading scores with six.
- Unitrends in its first ODM was second in the features category, while overall being classified as a challenger.
- Commvault was second overall, like the previous ODM in 2014-15, and demonstrated a consistent above average performance in all categories.
- Dell remains a leader, but its software division has recently been sold off to a private equity firm, and will be relaunched under a new name on November 1.
- Actifio was classified as a leader in its first ODM and was second in terms of the number of leading sub-category scores with six.
- HPE slipped to challenger with only recording three sub-category leading scores.
- Asigra and Datto in their first ODM were both challengers, with Asigra recording four sub-category leadings scores, and Datto the leader in the execution category.
- Artisan in its first ODM was classified as a challenger but was the clear leader in the operational management sub-category.
- Arcserve was classified as a challenger and was the leader in the deployment and TCO sub-category.

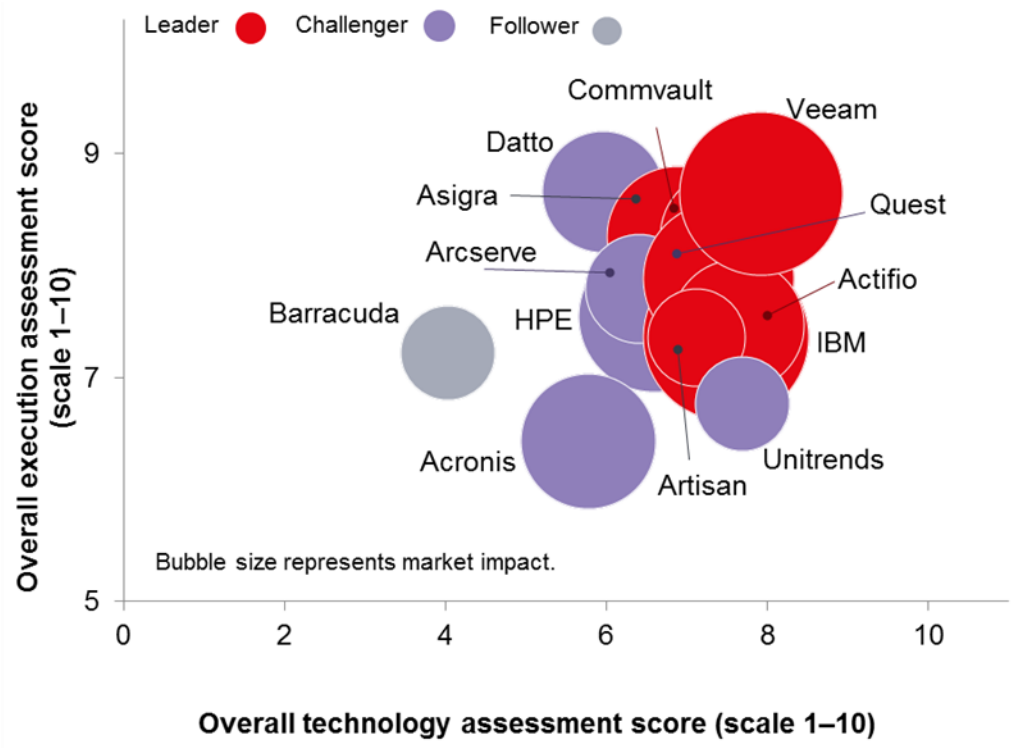
Market and solution analysis

Ovum Decision Matrix: Data Availability and Protection Solution for the Cloud Era, 2016-17

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. In fact, nearly 50% of the vendors are new entrants to the Ovum Decision Matrix, demonstrating how the market has changed. Today, the cloud has introduced a new layer of capability when it comes to data protection and availability. The 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. The difference from the previous ODM 2014-15 is that Veeam has taken over

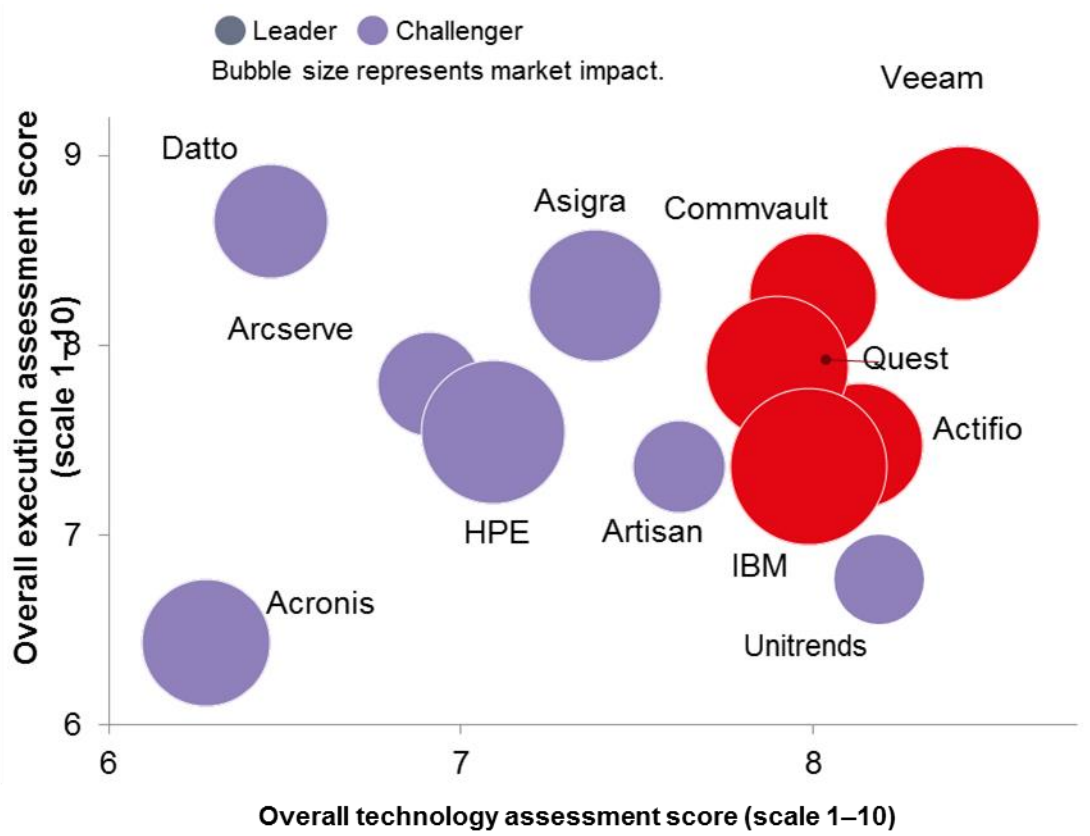
as the clear leader, with Commvault retaining its position as second overall. The other leaders are a mix of established vendors and newer vendors with solutions designed and built in the cloud. The interesting feature of this report is that, despite the four-month notice of the production schedule for the report, two of the previous leaders (Symantec now Veritas, and EMC now Dell) despite the four-month notice of the production schedule for the report choose not to participate.

Figure 1: Ovum Decision Matrix: Data Availability and Protection Solution for the Cloud Era, 2016-17



Source: Ovum

Figure 2: Expanded view of Ovum Decision Matrix: Data Availability and Protection Solution for the Cloud Era, 2016-17



Source: Ovum

Table 1: Ovum Decision Matrix: Data Availability and Protection Solution for the Cloud Era, 2016-17

Market leaders	Market challengers	Market followers
Actifio	Acronis	Barracuda
Commvault	Arcserve	
Dell	Artisan	
IBM	Asigra	
Veeam	HPE	
	Unitrends	

Source: Ovum

Market leaders: Actifio, Commvault, Dell, IBM, and Veeam

The leaders in the Ovum ODM on Data Protection and Availability in the Cloud era all scored a normalized average across all three categories of over 7/10. However, the leader category is characterized by two different groups of vendors. Veeam, with a score of 7.9/10 was the clear overall leader, with Actifio, Commvault, Dell, and IBM in a group with an average score of 7.24/10. Within this leadership category, vendors such as IBM performed extremely well in some sub-categories. IBM was the leader with six sub-category leading scores, compared to other leaders such as Dell that recorded only one sub-category leadings score. This variation demonstrates that while on average the leaders

performed well, it was a mixture of those that were more consistent, and those that excelled in some sub-categories and by implication did less well in others.

Market challengers: Acronis, Arcserve, Artisan, Asigra, Datto, HPE, and Unitrends

The challengers demonstrated a consistent scoring record being on or just above the average for the different categories (features, execution, and market impact). 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. Acronis's performance was mixed, but in terms of technology capability it was particularly strong in terms of all aspects of data management and DR, and replication. Arcserve scored below average in operational management, data management, and security in the features category, while Artisan scored below average in the platforms, security, and backup and recovery sub-categories. Asigra was weak in DR and replication and deployment and TCO sub-categories. Datto performed very well in execution and market impact but recorded the second lowest average score for features overall. HPE was impeded by poor scores in the security and deployment and TCO sub-categories, and if these scores had been in line with the average, HPE would have remained a leader. However, Unitrends scored in line or above average for the features category, but was impeded by four scores in the execution and market impact categories that were below average. The key differentiator between the challengers and the leaders was seen in the lack of some features, but was most apparent in market impact where the majority of challengers (all except Asigra and HPE) scored below average for two of the sub-categories. This shows that while the challengers have solid products that can match the leaders in at least 75% of cases, the products do not have the wider market appeal to enable the challengers to develop wider market opportunity/recognition and be ranked as a leader in Ovum's ODM.

Market followers: Barracuda

With such a mature market the category of followers is small, with only Barracuda ranked in this section. The key differentiator between is that all Barracuda's features scores were below the average for the companies evaluated in this report. This demonstrates that while Barracuda has a viable and comprehensive solution it lacks some of the additional features. In terms of execution Barracuda was in line with the average, demonstrating that it has the ability to meet the execution needs of organizations. However, Barracuda was also categorized as below average in the market impact category, with a less balanced market where not all verticals or markets were served equally.

Emerging vendors

Table 2: Emerging vendors: Data Availability and Protection Solution for the Cloud Era, 2016-17

Vendor	Product
CloudEndure	CloudEndure Disaster Recovery & Live Migration
Dattos IO	Datos IO RecoverX
iland	iland Disaster Recovery-as-a-service

Source: Ovum

CloudEndure

The approach taken by CloudEndure is that by continuously replicating the current application stack and then automatically converting the application on the target location, it can be migrated to a different environment with no data loss, no performance disruption, and no manual configuration. While this is true it is still not yet a nirvana, but works for operating environments including Linux (Ubuntu, Red Hat, CentOS, SUSE Linux, Amazon Linux, Oracle Linux, Debian Linux, Kali Linux) and Microsoft Windows Server 2003, 2008, 2012 (all 32/64 bit, including R2). CloudEndure also supports AWS, Microsoft Azure, Google Cloud Platform, OpenStack, VMware, and CloudStack environments. The big advantage of the CloudEndure solution is that its replication includes all the aspects of the operating environment, including the attached storage, network topology, and IP address. These are automatically recognized and replicated so the application can run immediately in the cloud environment.

The CloudEndure solution portfolio has two products: CloudEndure Disater Recovery and ClouldEndure Live Migration. These products share some common traits in that to operate, both require agents to be deployed on the source machines, and both have the concept of non-disruptive testing of a cutover (in the case of migration) or a failover (in the case of disaster recovery). Ovum believes this testing capability is a key benefit that is often undervalued. The ability to test and confirm that the primary and secondary environments are synchronized is an important auditable requirement if trust in any DR provision is to be extended to business users.

CloudEndure disaster recovery

The idea that any disaster can be mitigated by a backup site within a metropolitan area was challenged by Hurricane Katerina, where primary and secondary data centers were destroyed over a 100km area. CloudEndure enables replication between a wide variety of environments, so that an organization can select AWS as its DR location and with a single click failover from the live running site to the DR site that might be many hundreds of miles away.

CloudEndure live migration

The portability of workloads between cloud providers has always been a challenge, with many public cloud environments having proprietary hooks that make migration a time-consuming task. CloudEndure captures a block-level replica of the entire application stack and its environmental configuration irrespective of if it is operating in a physical, virtual, or cloud environment. Its continuous data protection technology enables migration with very short cutover windows, providing businesses with little or no performance disruption.

Datos IO

The value proposition of Datos IO RecoverX is that it is designed and built for scale-out databases so that these can be protected and recovered to a point in time. Datos IO RecoverX is for four specific use cases initially: cloud-native backups, long-term data retention, data portability, and multi-cloud environments. The challenge with a scale-out architecture such as with cloud databases is that it requires a fundamentally different backup architecture and approach to protect data in databases, and Datos IO has developed two main capabilities specifically for this task.

Consistent orchestrated distributed recovery

Datos IO has a consistent orchestrated distributed recovery (CODR) engine as the core technology to manage the challenges of backing up the scale-out databases used by cloud-native applications. The

challenge with these new distributed scale-out applications is that the data is spread across commodity hardware, and has the ability through clustering technology to survive any single node failure. This approach provides a very resilient solution, but also provides new challenges for backup and recovery. Because the data is highly distributed and the databases provide resiliency, it has been suggested that backup is redundant for these environments. The issue is that the strength of these environments is also their weakness, because any corruption of the data can quickly spread across all replicas, and without point-in-time backup and recovery, the corruption could be terminal.

To meet the needs of this market, CODR uses database-specific stateless agents. These agents, or listeners in Datos IO speak, identify any change in the application and transmit in parallel the data to a backend data store. However, to make this data usable it is further de-duplicated and reassembled to represent a consistent representation of the source data.

Semantic de-duplication

Semantic de-duplication, an industry-first approach, is designed to reduce the cost of storing backups of distributed databases. The current approach to the backup of these scale-out databases is to keep multiple copies of full backups from these databases, and keep these copies for as long as the governance policies dictate data retention. Datos IO uses versioning so that only a single copy of the databases needs to be kept, and sematic de-duplication is used to compute a cluster-consistent view of this data in a single copy.

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 companies have little confidence in should they need it. iland's DRaaS solution combines the four principles and is also a cost-effective solution to help organizations reduce the overhead costs associated with setting up and managing a DR plan.

Security

The general concern of many CIOs is that the cloud is inherently less secure than an on-premise solution. ICT Enterprise Insights 2015/16 – Global: ICT Drivers and Technology Priorities, n=4,676 discovered that 55% of respondents put managing security as one of their top three challenges for 2017. iland includes in its DRaaS offering an array of security features including vulnerability scanning, encryption, anti-virus, and anti-malware protection as part of the service, which is fully managed by iland's security team. A comprehensive monitoring capability covers the integrity of the data, and also extends to cover web reputation monitoring, with cover to block any denial of service attacks also provided.

Support

A central capability for most organizations adopting cloud services is the availability of 24x7 regional support, and the professional services that can help with the adoption of the cloud. iland has developed a support infrastructure and a team of architects that help organizations smooth the adoption of these services and ensures 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 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 challenged by Hurricane Katrina in the US, where primary and secondary data centers were destroyed over a 100km area. Even greater 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. The data centers are all tier-3 rated, and many have tier-4 capabilities, such as guaranteeing 99.982% availability, but because of their location cannot be classified as tier-4.

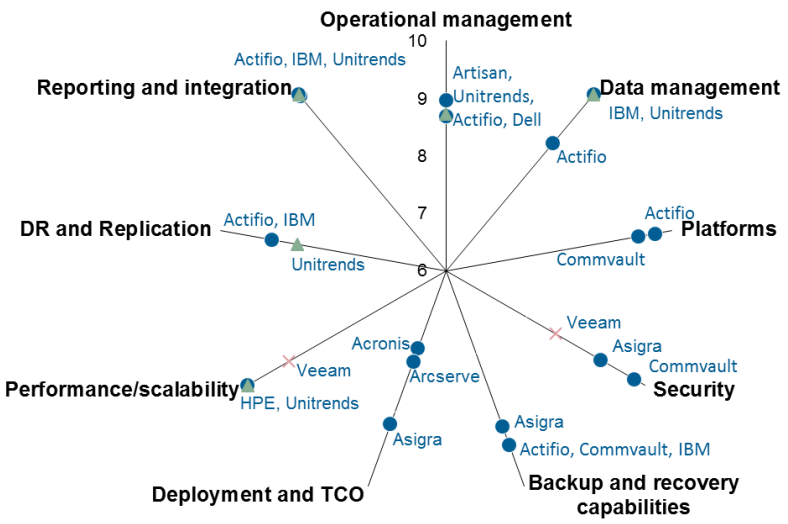
Integrated management

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 running costs of the 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.

Market leaders

Market leaders: technology

Figure 3: Ovum Decision Matrix: Data Availability and Protection Solution for the Cloud Era, 2016-17 – Market leaders – technology

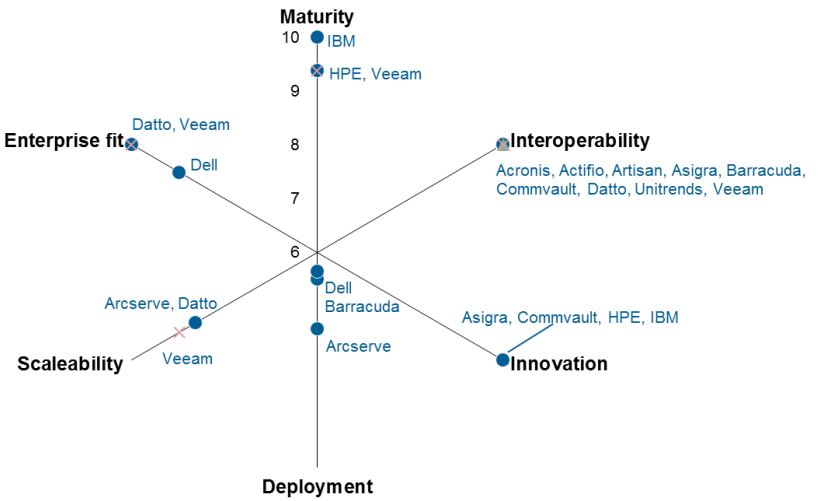


Source: Ovum

Figure 3 shows the top three vendors by sub-category. While Veeam was the overall technical capabilities market leader, it only recorded two entries in the market leaders diagram: performance and scalability and security. The leading vendor was Actifio with six sub-category entries on the technical capabilities market leaders diagram: reporting and integration, operational management, data management, platforms, backup and recovery, and DR and replication. This demonstrates that overall Actifio has significant strength in areas that relate to the management aspects of data availability. Unitrends, with five sub-category entries on the market leaders diagram (reporting and integration, operational management, data management, performance and scalability, and DR and replication) shows the strength of its providing a recovery guarantee. IBM was third on the list with four sub-category entries on the market leaders diagram (reporting and integration, data management, backup and replication, and DR and scalability) which fits with the fact it was IBM services that submitted its entry in the ODM. Commvault and Asigra recorded three entries each, with security a joint strength. Acronis, Artisan, Arcserve, and Dell complete the leaders diagram with one entry each. The diagram demonstrates that all the vendors have some key differentiating capabilities, matching vendors to requirements is essential to obtaining the best possible shortlist of vendors.

Market leaders: execution

Figure 4: Ovum Decision Matrix: Data Availability and Protection Solution for the Cloud Era, 2016-17 – Market leaders – execution

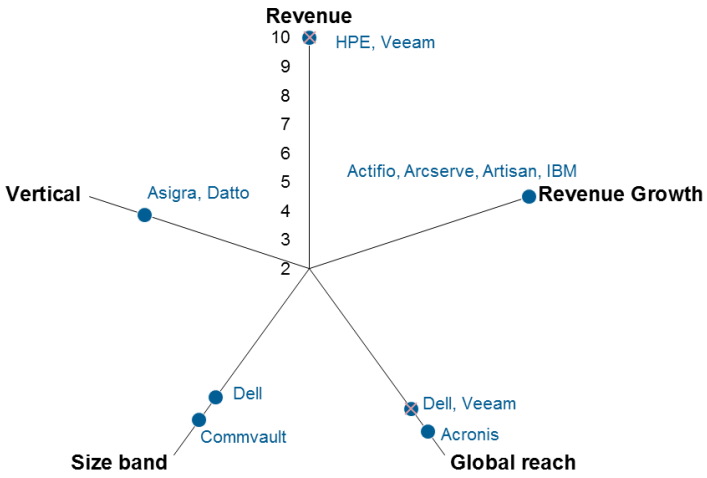


Source: Ovum

In terms of execution Datto was marginally the leader with an average score of 8.65 out of 10 compared to Veeam that was second with 8.64. Datto, however, had three market leading entries compared to Veeam's four. Datto was strong in enterprise fit, scalability, and interoperability, while Veeam was strong in enterprise fit, scalability, interoperability, and maturity. Arcserve, Barracuda, Commvault, Dell, and HPE all recorded two market leading entries, while Acronis, Artisan, Asigra, and IBM complete the leader board with one entry each.

Market leaders: market impact

Figure 5: Ovum Decision Matrix: Data Availability and Protection Solution for the Cloud Era, 2016-17 – Market leaders – market impact



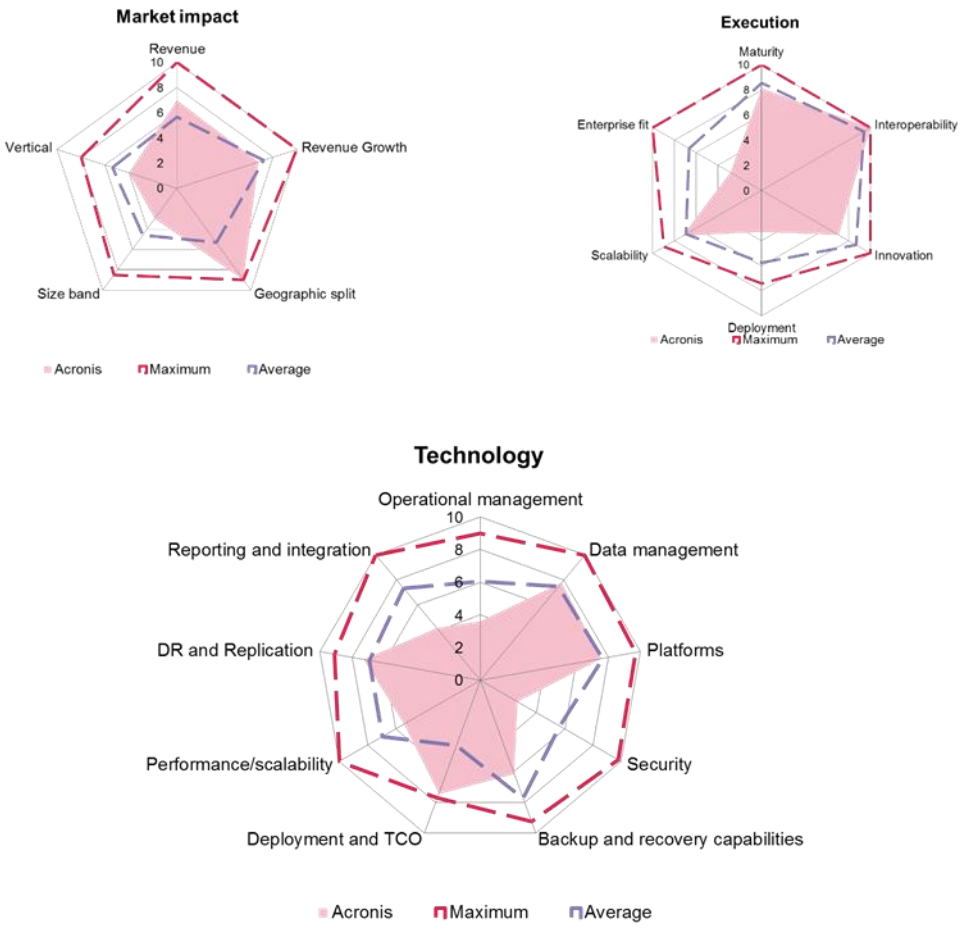
Source: Ovum

In the market impact category Veeam was the overall market leader, with Dell and HPE in joint second. Only Dell and Veeam recorded more than one market leading entry, with Acronis, Actifio, Arcserve, Asigra, Artisan, Commvault, HPE, and IBM completing the leader board with a single entry each. HPE and Veeam were the financial giants in the market, while Actifio, Arcserve, Artisan, and IBM were the fastest growing vendors. Acronis and Dell had the most balanced global reach, with Commvault and Dell having the most balanced customer profile in terms of size band. Asigra and Datto were equally balanced when it came to market vertical coverage.

Vendor analysis

Acronis (Ovum recommendation: challenger)

Figure 6: Acronis radar



Source: Ovum

Products assessed in ODM

Acronis Disaster Recovery Service

ODM assessment

Acronis's performance was mixed, and in terms of technology capability it was particularly strong in terms of all aspects of data management and DR and replication where it scored in line or above the average. It was also strong in terms of deployment and TCO where it was one of the leaders in that sub-category, with one of the lowest support and maintenance costs. Acronis's other noteworthy strength was in the range of platforms supported. In terms of the market impact Acronis was in line or above average for 60% of the capabilities, with good revenue and above average revenue growth across a balanced geographic market. Acronis was in line or above average in 50% of the execution capabilities, and particularly strong in terms of interoperability and scalability. Ovum considers Acronis to be a solid performer with some excellent capabilities that needs to form a partnership or develop some security capabilities that can match those of its competitors.

Ovum SWOT assessment

Strengths

Eliminates the cost and complexity of performing a disaster recovery plan

The traditional approach to data protection relies on taking a master backup and then incremental backups. This means that restoring to a known point in time means recovering in a sequence, which can take many hours to complete. Acronis disaster recovery service uses a different approach, however, taking snapshots as frequently as every 15 minutes that can be transferred to the Acronis cloud directly or to a local appliance and then secured off-site.

Provides an automated disaster plan testing capability

The ability to know with confidence that any disaster recovery plan can be used when needed is a critical aspect of any DR plan. Acronis provides an automated DR testing capability so that organizations can test the DR plan without impacting normal business operations. DR testing usually involves taking the production system off line for a weekend and then entering test transactions to prove it is operational.

Weaknesses

Using the cloud for DR is not new but may still put off some traditional companies

The lack of a physical tape that holds the corporate data, and a set schedule for when a backup takes place requires new thinking about how corporate data is managed. The Acronis approach protects the data but requires the organization to be at a level of maturity in terms of its journey to become a digital enterprise, and could fail to resonate with traditionalist organizations. However, Ovum does expect that in the next two to five years this approach to data management will become more mainstream.

Opportunities

Develop partnerships with more public cloud providers

The cloud is not a single entity, and the number of different providers continues to expand to meet local data protection regulations. Acronis needs to build more partnerships so that its service can be deployed in any geography.

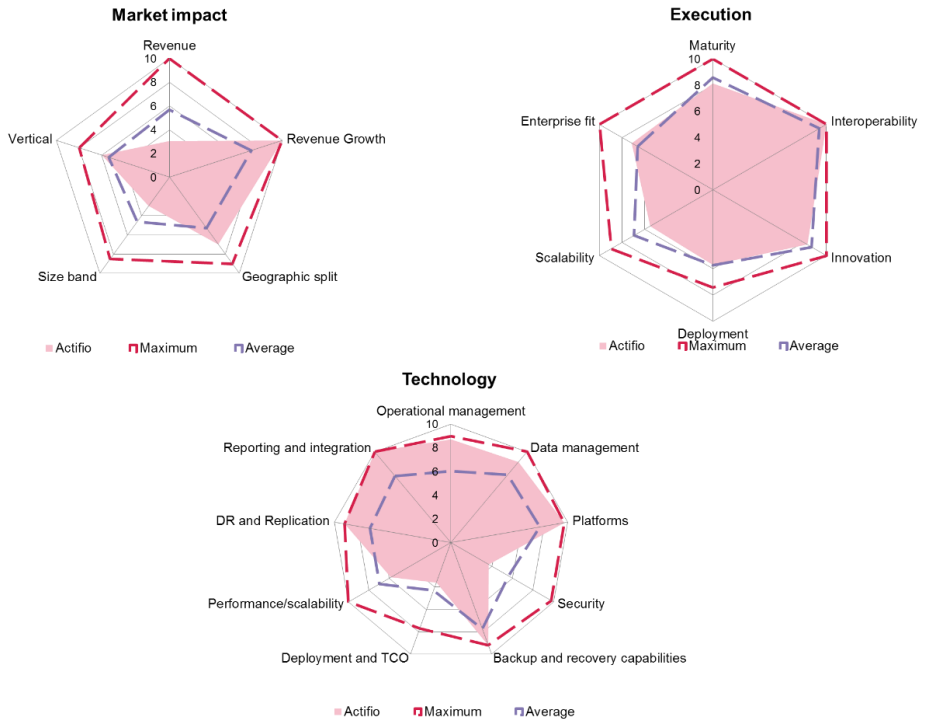
Threats

The local data protection regulations make the cloud appear an unsuitable solution

The whole concept of cloud data protection and availability could be impacted by local data protection regulations/sovereignty. However, for Acronis this is less of a threat because it allows organizations to use a local appliance as a target. Ovum believes this threat will therefore impact only part of the Acronis service and will be less of an issue for Acronis than it is for some of its competitors.

Actifio (Ovum recommendation: leader)

Figure 7: Actifio radar diagrams



Source: Ovum

Products assessed in ODM

Copy Data Virtualization v7.0

ODM assessment

Actifio recorded five leading sub-category scores across all three categories, and was particularly strong in execution and technology categories. In terms of execution, Actifio was in line or above the average in all but one of the sub-categories, and was particularly strong in interoperability. In the technical category, Actifio recorded a mixed performance, but in terms of DR and replication, reporting and integration, operational management, data management, platforms, and backup and recovery it was either a leading score or well above average. In terms of market impact, Actifio was a leader in terms of revenue growth and above average for both geographic and vertical market segmentation, meaning it has a balanced portfolio of customers. Ovum believes that in its first ODM appearance, Actifio has performed excellently, being in the leader classification against much bigger and more established competition.

Ovum SWOT Assessment

Strengths

Reduces impact on production applications

Actifio takes an incremental forever data ingestion approach, which significantly reduces storage and network IO on production applications, enabling them to perform better. For very large databases (VLDBs) and large NAS filers with hundreds of millions of files, Actifio's incremental forever approach

keeps the backup window very small, which is something that every DBA and backup admin approves of.

Eliminates the cost and complexity of restoring data to a known time

The traditional approach to data protection relies on restoring a full backup and then applying incremental images, all of which increases the recovery time objective (RTO). Actifio uses a different approach and provides instant recovery for everything including VMs, VLDBs, physical servers, and NAS filers by provisioning point-in-time virtual copies and reducing application downtime.

Flexible dial for RTO, RPO, and retention reduces total cost of ownership

With centralized and simple SLA management for various application tiers, Actifio enables users to specify RTO between five minutes and 24 hours, RPO between one hour and 24 hours, and Retention between hours and decades. This enables enterprises to replace multiple point tools such as backup, de-duplication, replication, DR orchestration, and test data management for DevOps to reduce the total cost of ownership.

Self-service and fast data access for test and development

Actifio provides the ability to instantly provision multiple virtual copies of production application data in dev, QA, UAT, and production support test environments in a self-service way. This helps enterprises uses backup copies to accelerate their application release cycles and improve product quality by catching defects early in release cycles.

Data availability anywhere

Actifio software enables enterprise IT to deliver functionalities including backup, DR, and test data management on any storage or compute anywhere, such as a private cloud, public cloud, or any of the 60 or so managed service providers that are using Actifio platform.

Weaknesses

This new approach to data protection may put off some traditional companies

The lack of a physical tape that holds the corporate data, and a set schedule for when a backup takes place requires new thinking about how corporate data is managed. The Acronis approach protects the data but requires the organization to be at a level of maturity in terms of its journey to become a digital enterprise, and could fail to resonate with traditionalist organizations. However, Ovum expects that in the next two-five years this approach to data management will become more mainstream.

Opportunities

To build integration points with key new organizations developing DevOps solutions

Large financial institutions have integrated Actifio via APIs into continuous integration (CI) tools such as Ansible and Jenkins. Ovum believes that many enterprises in multiple verticals could benefit if Actifio comes up with out-of-the-box integration with popular DevOps tools.

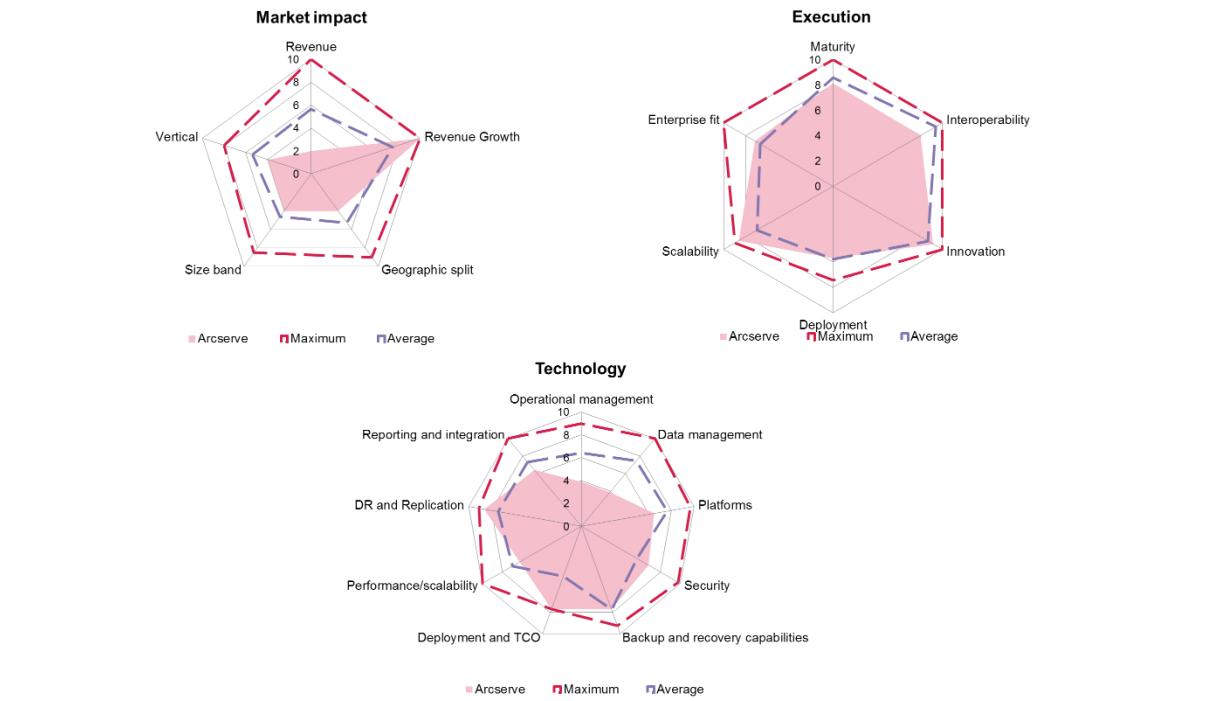
Threats

The bigger incumbent vendors acquire similar technology

The data protection and availability space is a rapidly changing market. Actifio has to balance the need to develop its solution with its budget, because if a larger competitor were to acquire one of its competitors it could alter the market dynamics.

Arcserve (Ovum recommendation: challenger)

Figure 8: Arcserve radar diagrams



Source: Ovum

Products assessed in ODM

Arcserve Unified Data Protection

ODM assessment

Arcserve demonstrated a solid technical capability backed by an excellent execution capability, with an average market impact performance. In terms of execution, Arcserve was in line or above the average for five out of the six sub-categories, and only just below the average in the sixth. From a technology perspective, Arcserve was in line or above average for platforms, security, backup and recovery, deployment and TCO, performance and scalability, DR & replication, and reporting and integration. Arcserve was noteworthy as one of a handful of products that could be deployed by a single FTE in under an hour. Arcserve was weaker than the average in operational management due to the product enhancements not being ready for this ODM. In terms of market impact, Arcserve was the leader in terms of revenue growth, indicating that its solutions are resonating with the market demand.

Ovum SWOT Assessment

Strengths

Enable IT generalists to set up and operate any data protection plan

The traditional approach to data protection relies on experienced IT specialists to implement, configure, and manage the process of protecting data assets. Arcserve has developed a simple UI that allows non-specialist IT staff to provide this service, and the introduction of wizards has also enabled these solutions to be deployed and installed by non-specialist IT staff.

Reduces the storage costs associated with data protection

The de-duplication algorithms used by Arcserve enable it to confidently quote a sizing ratio that takes into account storage reduction of 3X over the lifetime of the appliance, meaning a 90TB backup source will only require 30TB of raw target storage over time. Arcserve says its de-duplication capabilities differentiate it from others in the market because it is global and source-based in its de-duplication, and not just job-based like many of its competitors.

Supports VMware Virtual Volumes

Arcserve UDP supports VMware vSphere version 6, and in particular Virtual Volumes (VVOL). VVOL provides administrators with the ability to manage each VM as an individual entity, and enables them to modify its storage characteristics individually in line with changing business or operational requirements.

Provides a continuous available capability

Arcserve combines its different technology capabilities to provide organizations with a continuous available promise for data and services. This capability provides continuous replication and full-system high availability of physical and virtual systems for both Windows and Linux. Ovum particularly likes the ability to protect the hypervisor environment itself as well as application-level failover and failback.

Weaknesses

No Linux-based virtual appliance

The portfolio of solutions is missing a Linux-based virtual appliance that could be deployed on OpenStack. Ovum understands that a Linux virtual appliance is on the roadmap for development, which should address this gap. OpenStack is rapidly becoming a platform of choice for service providers and enterprise organizations alike.

Opportunities

To expand its footprint in North America

While Arcserve is headquartered in Minneapolis, for historical reasons most of its business is based in EMEA and Japan. Arcserve with its US heritage and headquarters is in an excellent position to grow its customer base in North America, which is easier than a US vendor trying to expand in EMEA which is a more complex market.

Threats

The cost of raw storage becomes cheap enough to erode the value of de-duplication

The cost of raw storage is declining on a per GB basis, but is still not cheap enough for organizations to not care about reducing the volume of data they have to protect. If the cost of storage falls too low, organizations will re-evaluate their approach to storage and this could impact Arcserve in terms of the value organizations put on its de-duplication technology.

Artisan (Ovum recommendation: challenger)

Figure 8: Artisan radar diagrams

Source: Ovum

Products assessed in ODM

Artisan Neverfail HybriStor

ODM assessment

Artisan's performance was solid across the range demonstration of its capabilities. Artisan was strong in terms of its technology capabilities with scores in line or above average for operational management, reporting and integration, DR and replication, performance and scalability, data management, backup and recovery, and security. Artisan's noteworthy strength is that a single FTE administrator can manage and configure more 10PB of data, which has massive implications for IT operational support costs. Artisan was in line or above average for four of the six sub-categories in the execution category with interoperability being a significant strength. The market impact performance was more mixed. Artisan was a leader in the revenue growth sub-category demonstrating its future impact, and while being balanced from a vertical and size-band perspective in terms of customers, the geographic balance was lower than the average due to a larger proportion of customers in the Americas.

Ovum SWOT Assessment

Strengths

Enable IT storage analyst to simply manage the data protection process

The traditional approach to data protection relies on experienced IT specialists to implement, configure, and manage the process of protecting the data assets. Artisan has employed a simple NAS

management approach that will be familiar to all storage analysts and is common across all the data being protected, irrespective of where it is held.

Reduces the storage cost associated with data protection

The de-duplication algorithms used by Artisan enable it to reduce the raw storage needed compared to its competitors. Artisan says its de-duplication capabilities differentiate it from others in the market because it is global in its de-duplication, and not just job-based like many of its competitors.

Reduces the recovery time

Artisan has developed a technology called InstaCache that enables the data to be automatically recovered from the more cost-efficient de-duped storage to fast-performing SSD storage for local and remote near-instant data recovery.

Weaknesses

A hardware purchase in an increasingly software world?

Artisan is an appliance-based solution which fits the need of its customers. However, the move from organizations is toward a software-focused purchasing approach, which means the sale-to-cash cycle for an appliance is longer.

Opportunities

Build a better brand awareness message

Artisan acquired NeverFail in 2014 and has been integrating the two companies and building its reputation as an integrated data protection vendor. However, it be would be fair to say that it has only just recently developed a clear branding approach that resonates with existing and potential new customers. Ovum believes that the Artisan NeverFail approach blends the core values of both companies into a single message, but more work is needed to exploit these values.

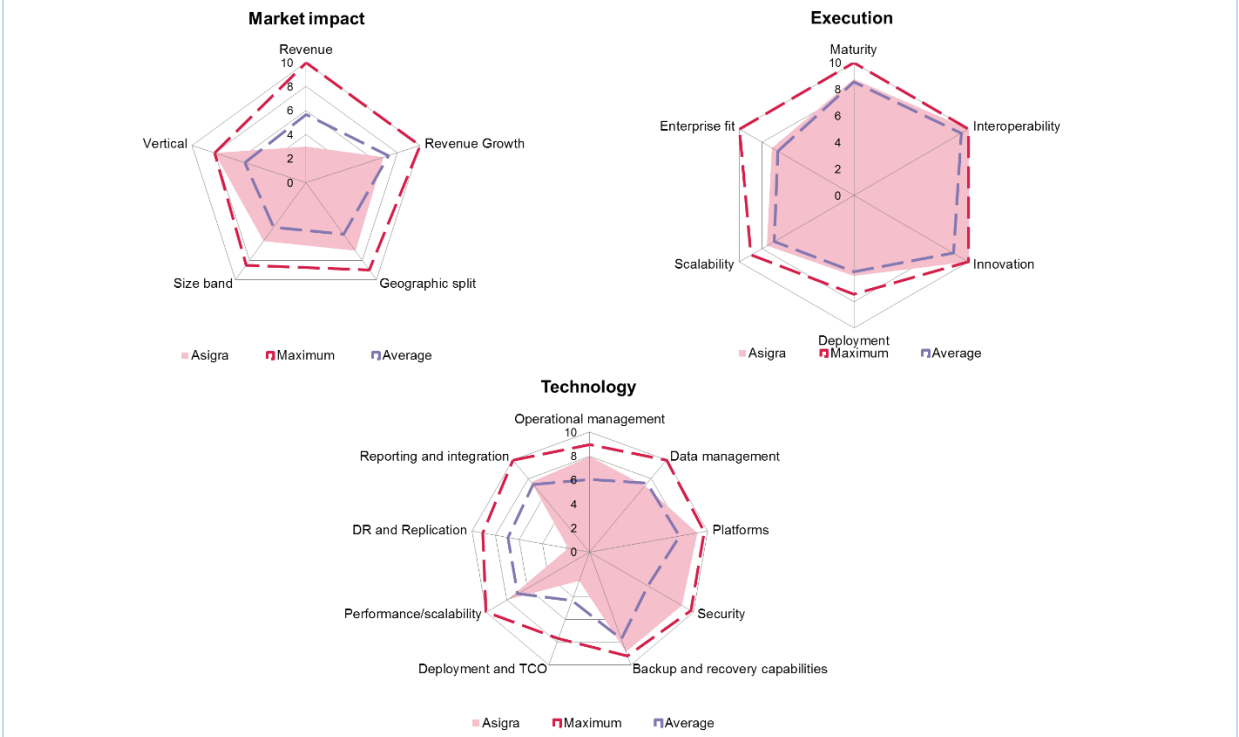
Threats

The cost of raw storage becomes low enough to erode the value of de-duplication

The cost of raw storage is declining on a per GB basis, but is still not inexpensive enough for organizations to not care about reducing the volume of data they have to protect. If the cost of storage falls too low, organizations will re-evaluate their approach to storage and this could impact Artisan in terms of the value organizations put on its de-duplication technology.

Asigra (Ovum recommendation: challenger)

Figure 9: Asigra radar diagrams



Source: Ovum

Products assessed in ODM

Asigra Cloud Backup v13.1

ODM assessment

Asigra showed a very strong performance in the execution category with all sub-category scores being in line or above the average. However, in the technology category, Asigra's performance was more mixed, but it had significant strengths in operational management, platforms, security, and backup and recovery where Asigra was well above the average. The noteworthy capability from Asigra is that it is one of a small number of vendors that can ensure that data is only capable of being recovered to the originating device, which is an excellent security benefit. This can be overridden where needed but requires elevated privileges. In terms of market impact, Asigra was above average in four of the five sub-categories, demonstrating a balanced customer base with excellent revenue growth.

Ovum SWOT Assessment

Strengths

A revolutionary approach to licensing its solutions

The cost of data protection is traditionally based on the storage capacity consumed to hold the backups. However, it is the ability to recover data that is the critical aspect of any solution, and Asigra has developed a new licensing model that is based on the percentage of data successfully recovered in a year. This approach is a better way of measuring the value of data protection because it is only when data is recovered that the organization sees the benefit of data protection.

Protects containers technology and can be deployed in a container

The rise of microservices and containers technology is a hot topic in 2016. Currently the management and protection of containers is provided by only a few software vendors. Ovum considers this to be a significant strength of Asigra and one in which it can develop a leadership position.

Weaknesses

The 100% channel and the focus on service providers may put off some companies

The business Asigra has developed is mainly based on the service provider market, where service providers use Asigra technology to offer cloud-based data protection services to customers. Ovum believes that Asigra needs to expand to SMB and enterprise customers to balance its customer base.

Opportunities

To build integration points with key new organizations developing DevOps solutions

While Asigra is not a DevOps solution, its approach and technology can be integrated into agile development processes and tools. Ovum believes that Asigra should consider licensing its technology to these specialist vendors, while also maintaining it messaging on its wider application.

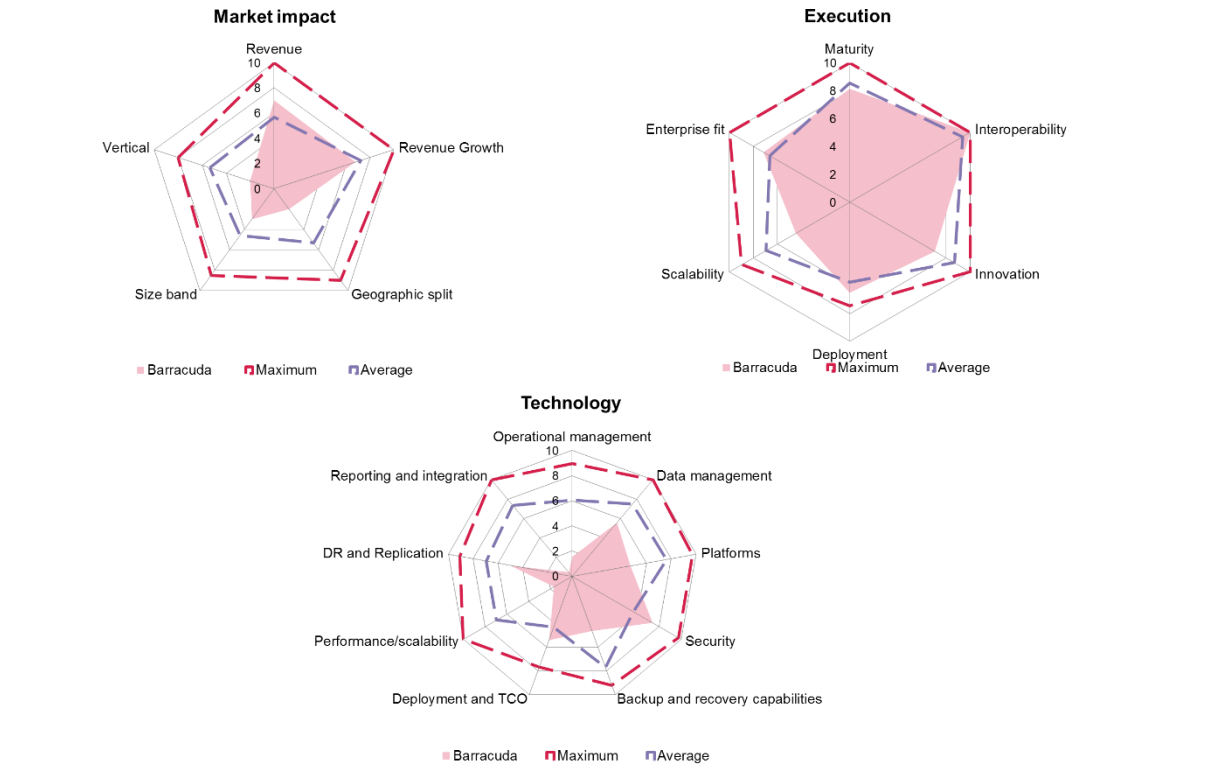
Threats

The service provider vendors acquire similar technology of their own

The data protection and availability space is a rapidly changing market. The service provider vendors in the market may decide to acquire a new start-up vendor to exploit its technology to drive its business. If this happens, the market dynamic could change and Asigra might have to move to a new operating model.

Barracuda (Ovum recommendation: follower)

Figure 10: Barracuda radar diagrams



Source: Ovum

Products assessed in ODM

Barracuda Backup v6.2

ODM assessment

Barracuda demonstrated a very good ability to execute, with four of the five sub-category scores close to or above average. Barracuda was noteworthy for its interoperability where it has full integration with open source and third-party solutions, a capability that ensures organizations can obtain maximum value from any investment. The other noteworthy strength of Barracuda was it was above average performance in terms of security. Ovum considers Barracuda to have a good solution that meets its target audience needs, but if Barracuda is to expand into new markets it will need to add some missing features that its competitors offer.

Ovum SWOT Assessment

Strengths

The ability to manage from a web browser all the different environments and data

The cloud-based management capability, which is available for those that select a cloud-based approach, allows organizations to have a single-pane-of-glass view of all its data protection activities. Ovum believes that the ability to have visibility from any location and manage all the devices and data connected to the cloud repositories is a particular strength of Barracuda.

A simple to understand pricing model

The simplicity of Barracuda's pricing makes it easy to purchase a suitable data protection solution, and the usage guides help customers to size the solution needed for their specific environment. Ovum believes that the different features and capabilities included, such as de-duplication, compression, and the ability to be application-aware, are all significant factors for organizations to consider.

Has strong public cloud credentials

Barracuda was recently recognized as the Winner of the 2016 Microsoft Azure Certified ISV Solution Partner of the Year and also hold a Microsoft Azure Certification and Microsoft-Gold Application Development status. Barracuda is also an Advanced Technology Partner for AWS.

Weaknesses

Does not currently support containers technology data protection

The rise of containers in 2016 looks set to become a dominant technology in the data center because it is likely to be used by software vendors as the primary method of deployment. While very few vendors have solutions to manage or protect containers, Ovum believes this will become a significant requirement in 2017.

Opportunities

Develop partnerships with microservices and container-based solution providers

The microservices revolution requires a completely new approach to data protection, availability, and movement. Barracuda with its cloud-based approach is a good fit for providing these new solution providers with tools that allow for this technology to be managed. Ovum does not believe a data management-only approach is viable, and that organizations will want to manage this new technology with a single tool that can provide all the management capabilities, including data management and application protection.

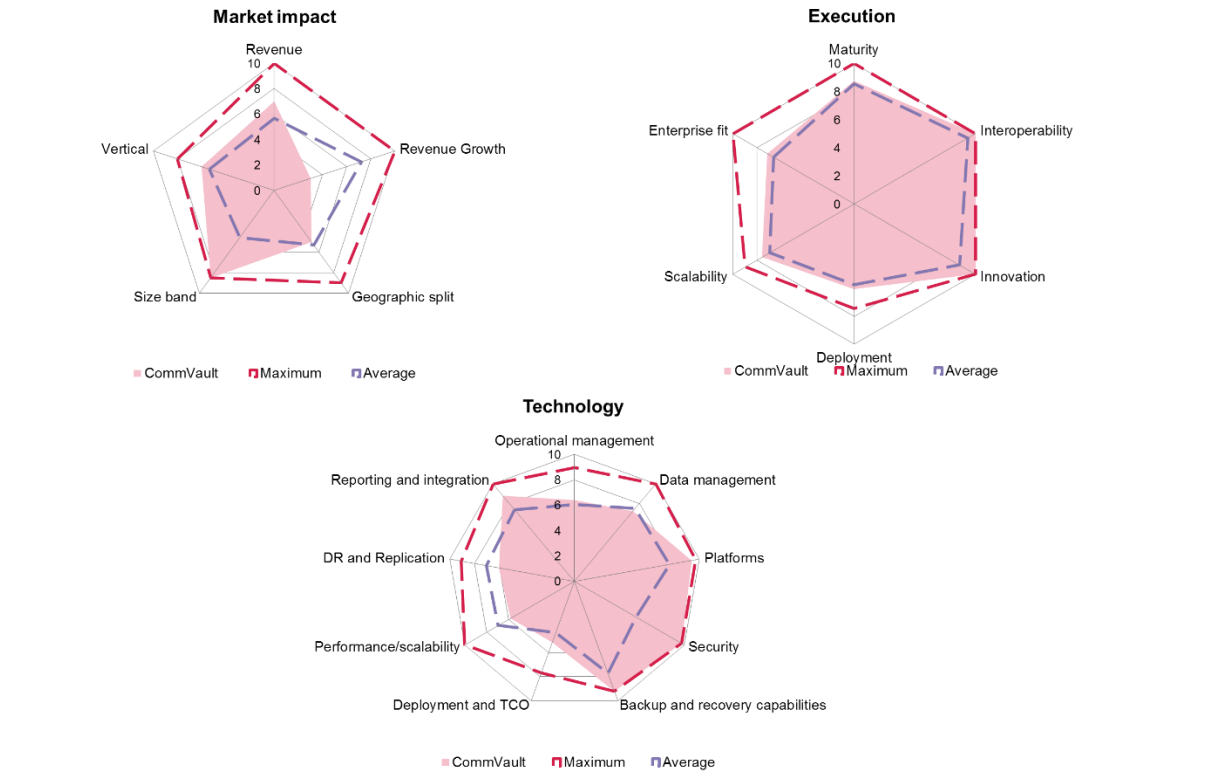
Threats

The Dell acquisition of EMC changes the market for physical appliances

The data protection and availability space is a rapidly changing market, and with Dell set to acquire EMC, the appliance market could become disrupted. Barracuda with its cloud approach does have a solution to challenge this, but it is the uncertainty in the market that is both a threat and an opportunity.

Commvault (Ovum recommendation: leader)

Figure 11: Commvault radar diagrams



Source: Ovum

Products assessed in ODM

Commvault Software, Version 11, Service Pack 5, released September 5, 2016

ODM assessment

Commvault overall was second in the ODM with an average normalized score of 7.6/10 compared to the leader with an average of 7.9/10. Commvault is also the most consistent vendor in the ODM, maintaining its position from the 2014/15 ODM. In terms of capability, Commvault's submission is based on currently available solutions, not to-be-released solutions like some of its competitors. Commvault's strength is its ability to execute, and here all six sub-categories were in line or above average. Ovum highlights Commvault's innovation and interoperability as key strengths of particular significance to organizations operating in a mixed hybrid cloud environment. In terms of technology, Commvault was in line or above average in all nine sub-categories, and particularly strong in terms of backup and recovery, security, platforms, and reporting and integration. One of Commvault's attributes only shared by a couple of vendors is the ability to make any data read-only to prevent unwanted copies being created. In terms of market impact, Commvault demonstrated a well-balanced customer portfolio across verticals, size-bands, and geographies and was above average in terms of revenue. Commvault's only area where improvement is required was in terms of revenue growth which was lower than the average, although the group has a mixture of smaller vendors that have high growth rates, and private companies that have no verifiable data points to confirm stated growth rates.

Ovum SWOT Assessment

Strengths

Eliminates the siloed approach to protecting data

The traditional approach to data protection encourages different teams to adopt specific solutions that work for their specific requirements. However, this approach has led to the fragmentation of the capability and creates a scenario where data protection becomes less efficient and reliable due to potential overlapping coverage and gaps in coverage. Commvault's platform approach allows a holistic view of all data to be seen, and protection plans to be developed accordingly.

Designed and built for the cloud era

The ability to work natively with a range of leading public cloud providers as well as different hypervisors enables Commvault to eliminate the complexity and performance degradation associated with on-premise gateways.

Integrates with the majority of leading storage and public cloud providers

Commvault has worked extensively with storage vendors to ensure its IntelliSnap capability can operate natively with the leading vendor's hardware-based snapshots, which reduces the overhead and greatly increases the options available to organizations.

Weaknesses

This platform approach could require professional services

The platform approach provides Commvault with the capabilities to solve the data protection challenges of organizations, but the audience must be able to see the holistic benefits. Ovum believes that Commvault needs to help CIOs position the platform to internal teams, otherwise internal resistance could derail any opportunity.

Opportunities

To expand the DevOps/SecOps applicability to new market verticals

While Commvault is not a DevOps vendor, its solutions are applicable to the DevOps and SecOps market. Ovum believes that Commvault should consider how its solutions and messaging can be targeted to this audience, and should investigate if market-vertical opportunities exist to create new use cases.

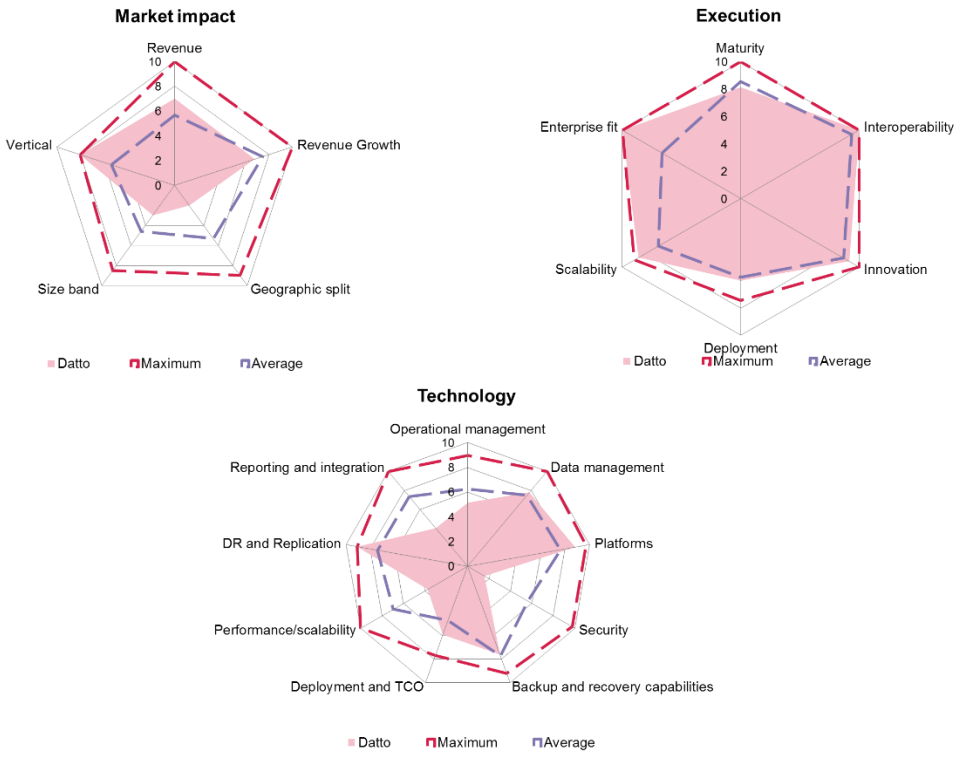
Threats

The number of applications that require specialist data protection increases

If the anticipated increase in the number of applications that require specialist data protection solutions such as Microsoft Office 365 happens, vendors will be faced with a challenge of when to develop these solutions.

Datto (Ovum recommendation: challenger)

Figure 12: Datto radar diagrams



Source: Ovum

Products assessed in ODM

SIRIS version 3

ODM assessment

Datto was very strong in terms of execution, where it exceeded the average score in five of the six sub-categories, and was in line in the sixth. Datto is particularly strong in terms of enterprise fit, where its roadmap is well defined and aligned to the needs of its target market. In terms of market impact, Datto has good revenues and revenue growth and a balanced spread of customers across the vertical markets, but is less balanced in terms of size-band or geography. Datto's position was ultimately determined by its technology scores which were mixed, with some significant strengths such as platforms, backup and recovery, DR & replication, and data management. Overall, Ovum places Datto as a challenger, and with more product or partner development in terms of capabilities, Datto has the ability to move toward a leadership position.

Ovum SWOT Assessment

Strengths

Eliminates the cost and complexity of restoring data to a known time

The traditional approach to data protection relies on taking a master backup and then incremental backups, so restoring to a known point in time means recovering in a sequence, which can take many hours to complete. Datto uses a different approach, inverse chain technology, where it takes an initial

copy and then builds a virtual copy of the original data in a time-stamped sequence, so recovery is as simple as mounting the data copy for the specific time stamp.

Can be restored to dissimilar environments

The ability to restore data quickly is a common requirement from customers, but the ability to restore to different environments is one that only becomes a requirement when needed. Ovum believes that Datto's ability to restore a bare-metal recovery to dissimilar hardware is a valued, if underrated, capability.

Datto creates a copy of the backup in the Datto cloud

The Datto solution allows organizations to automatically copy any backup to the Datto cloud. Users can control what gets copied to the Datto cloud, and also where the data is stored in the Datto cloud. Currently the Datto cloud is over 250 PBytes in size.

Provides a screenshot verification that a backed up application will boot up automatically

A backup is only of use if when needed it can be restored. Automatic verification that a protected application can be booted up from the Datto backup provides this. Ovum particularly likes the fact that the evidence via a screenshot is emailed to the administrator, and failures are alerted so immediate investigations can be performed.

Weaknesses

Only the data associated with containers can be protected

The ability to completely back up a container application is something that Datto cannot currently do. It does allow the data associated with a container to be protected, but not all the container's different layers. Datto plans to release this capability in 2017, which is when Ovum expects containers technology to begin to become mainstream.

Opportunities

To market the solutions as compatible with DevOps methodology and thinking

While Datto is not a DevOps solution, its approach and technology can be integrated into agile development processes and tools. Ovum believes that Datto should consider how to market its solutions to this segment of the customer base while retaining its messaging on its wider application.

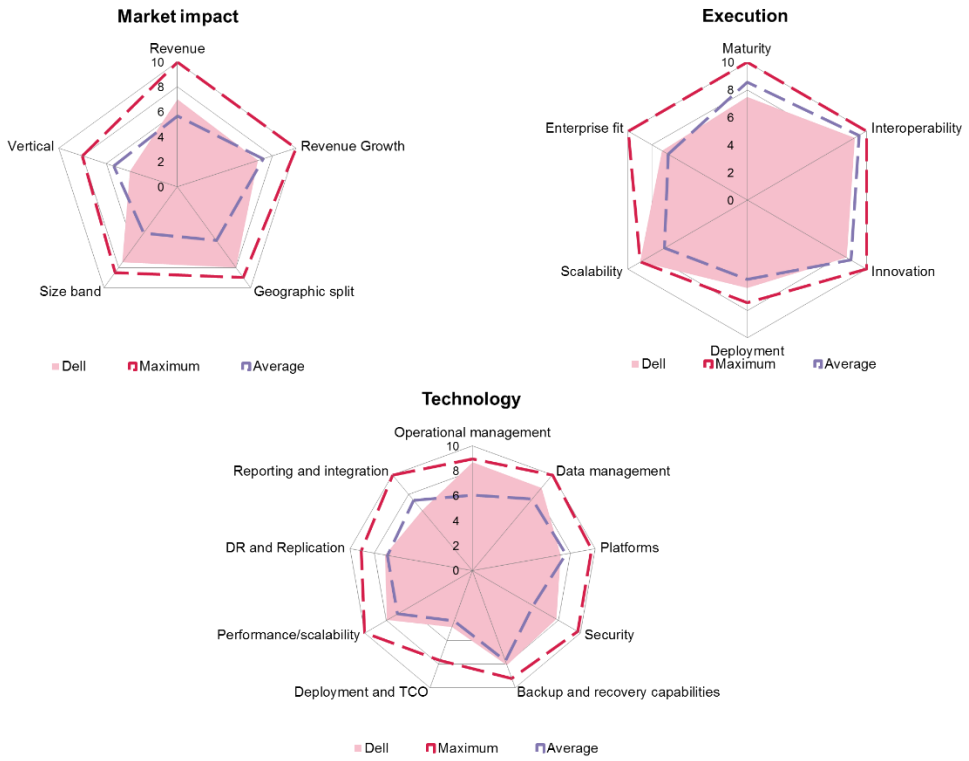
Threats

The market consolidates changing the economics for smaller vendors

There has not yet been any significant market consolidation in the data protection and availability space. The infrastructure market five years ago was similar and the Dell acquisition of EMC and the previous Lenovo/IBM sale has since seen the market consolidate. Ovum believes that the data protection market is ripe for consolidation, with large incumbent vendors with older technologies looking to bolster their position.

Dell (Ovum recommendation: leader)

Figure 13: Dell radar diagrams



Source: Ovum

Products assessed in ODM

Rapid Recovery version 6, and NetVault version 11

ODM assessment

Dell was a very close third in the overall ranking, with a 7.5/10 average score. It was one of the most consistent performers, scoring in line or above the average in 17 of the 20 sub-categories across all categories. Dell was joint second in the market impact category, where only its vertical market penetration scored below average. In terms of technology, Dell was one of the leaders in operational management, and also performed well above the average in the data management and security sub-categories. In the execution category, Dell scored in line or above average in five out of the six sub-categories, and was a leader in scalability sub-category. Dell's leadership in scalability was a result of its relatively low TCO for enterprise customers.

Ovum SWOT Assessment

Strengths

Minimizes the performance overhead of performing data protection

The traditional approach to data protection relies on taking a copy of the master data, whether a snapshot or a full backup, from the production environment. This puts an additional load on the production systems that causes performance degradation. Rapid Recovery's architecture means that this workload is offloaded to the "core", which is hosted on another server.

Any data can be recovered from anywhere at any time and a live VM can be executed directly from the backup

The major requirement of any data protection solution is the ability to recover data at any level of granularity at any time and in any location. Rapid Recovery with its "core" technology allows for each application to have its own core, and a single UI can manage all the cores of an organization. This approach also provides the added benefit of providing verification that the data is not corrupt as well as the ability to run a live VM from the backup without the need to restore it.

Provides native support for public cloud environments

Rapid Recovery provides native support for Microsoft Azure, and support for AWS and Google cloud is expected to be available shortly. Native support for public clouds allows VMs to be spun up or bare metal recovery to be performed, and Rapid Recovery also comes with built-in compression and de-duplication.

Weaknesses

Does not back up all of the data associated with a container

Like most solutions on the market, Rapid Recovery can protect the data lakes that sit behind containers, but does not protect the different layers of information contained within the container itself. This is a common issue, and for Rapid Recovery's target market, Ovum does not consider this too much of a problem. According to Ovum's research, most mid-market organizations do not plan to have a containers strategy until mid-2017, when Dell says support will be available.

Opportunities

To maximize the neutral position of the new independent company in providing holistic data protection

The strength of Dell's solution is based on its heritage and position in the market. As a newly independent software company, it can now claim infrastructure neutrality, which is a key difference from its previous offerings. Ovum considers this new flexibility to be a significant asset and one that needs to be exploited.

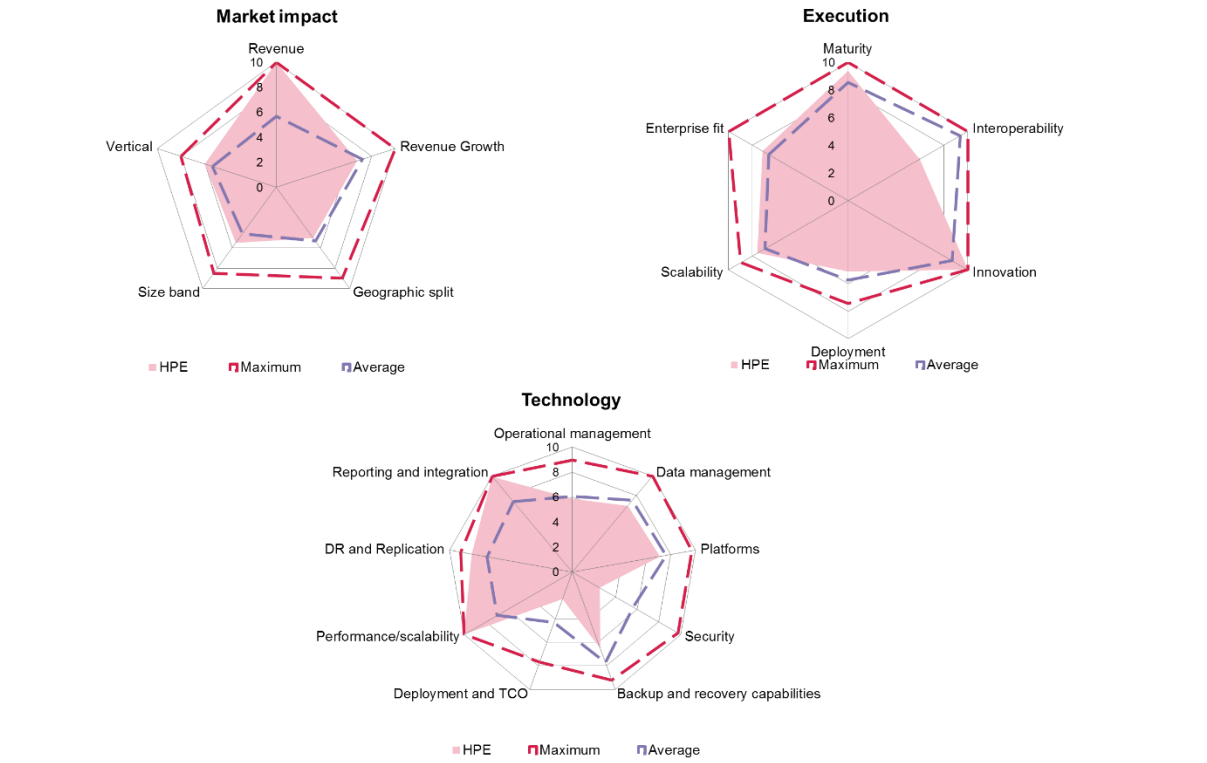
Threats

The brand awareness of the new independent company fails to gain traction

The big threat to any rebranding or de-merger exercise is that the marketing must ensure that the new brand retains and grows its popularity. Ovum believes that Rapid Recovery has a good brand name, with the advantage that it has only been associated with Dell for a short time. Any new association with a new company would not therefore have a long history to contend with.

HPE (Ovum recommendation: challenger)

Figure 14: HPE radar diagrams



Source: Ovum

Products assessed in ODM

HPE Adaptive Backup and Recovery Suite: HPE Data Protector 9.07 (July 2016), HPE Backup Navigator 9.40 (June 2016), HPE Storage Optimizer 5.3 (June 2016)

ODM assessment

HPE slipped from the leader category in 2014/15 to being a challenger in this report, but Ovum believes this is due to a timing issue. HPE was let down in terms of technology by a weak score in security, but a recent announcement (GDPR September 2016) regarding its security capabilities appears to address this weakness. This was not included in the report due to the report cut-off date for submission being the end of August 2016. In terms of technology, HPE was in line or above average in seven of the nine sub-categories, and particularly strong in performance and scalability, DR and replication, and reporting and integration. In terms of market impact, HPE was joint second and scored above average for all sub-categories. In the execution category, HPE again scored well with five out of the six sub-categories in line or above average. Overall, Ovum considers that the timing of the report did not help HPE and Ovum cannot speculate on the impact of the recent announcements on the relative position of HPE, except that it would certainly improve its overage average score of 7.1/10 that meant it was classified as a challenger.

Ovum SWOT Assessment

Strengths

The use of advanced analytics

The biggest added value that HPE ABR offers organizations is the use of analytics to help and guide the IT administrators managing the data protection plans. Ovum particularly likes the ability to set a recovery time objective (RTO), and the HPE ABR will let administrators know if it is being achieved, and if not then tell what they need to do to achieve this SLA. The other key strength with the use of analytics is that it helps organizations understand the data they have, ensuring that only important data is protected and redundant data ignored.

Works across a wide variety of infrastructure not just X86

The typical organization does not just have one type of infrastructure, it is normally a mixture of old and new, and increasingly includes cloud environments. Ovum considers that being able to protect corporate data wherever it is stored is an important capability if an organization needs a single solution for all its data protection requirements.

Uses federated deduplication

HPE ABR provides a federated approach to the de-duplication of data that means it can be performed at any point in the data supply chain to deliver maximum performance and conform to any local governance policies.

Weaknesses

Backing up and recovering a container is possible but not straightforward

Unlike most of its competitors, HPE can back up and restore containers such as Docker, although the process is not straightforward and individual containers cannot be recovered.

Opportunities

Exploit the market uncertainty that is happening

HPE has gone through a reorganization in recent years but is now focused on delivering solutions that meet market demand. However, recent mergers and de-mergers in the market create an opportunity for HPE to exploit because customers might be uncertain about the status of their current suppliers and their future plans.

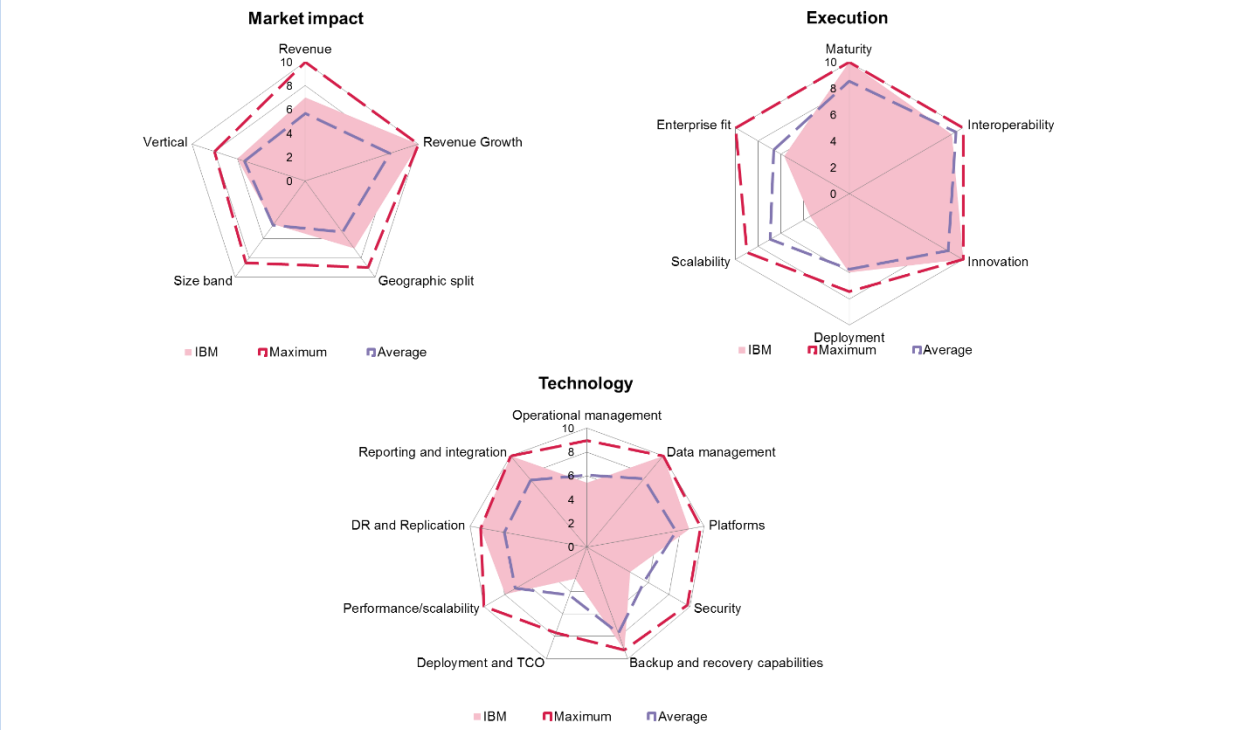
Threats

Organizations do not mature sufficiently in their adoption of automation technologies

While the first three stages of the HPE ABR solution offer excellent benefits, Ovum considers the final stage, automation, to be the level where maximum operational efficiency can be delivered. The concern is that organizations do not adopt the automation stage due to other internal pressures delaying the organization's growth in terms of the use of more machine-to-machine processing technologies. However, with the pressures IT organizations are facing, quickly adopting technologies that lessens management overhead is becoming a core requirement for survival.

IBM (Ovum recommendation: leader)

Figure 15: IBM radar diagrams



Source: Ovum

Products assessed in ODM

IBM Backup as a Service and IBM Disaster Recovery as a Service

ODM assessment

IBM scored in line or above average in all sub-categories in the market impact category, showing a well-balanced customer portfolio across verticals and geographies. In terms of execution, IBM score in line or above average in five of the six sub-categories, being particularly strong in terms of innovation and maturity. IBM's performance was mixed in the technology category, where it recorded four leading scores (reporting and integration, DR and replication, data management, and backup and recovery), three scores in line or just above the average (operational management, platforms, and performance and scalability), and two scores below average. The below average score from IBM is because IBM Resiliency Services based its responses on its managed backup and recovery services offerings. IBM was unable to respond to some questions in the ODM due to corporate policy. These included technology: deployment and TCO, execution: enterprise fit, and market impact: size band. In addition, there was a misunderstanding on some questions, including items in the technology security and execution and scalability sections. The lack of an IBM response here impacted the scores negatively.

Ovum SWOT Assessment

Strengths

Takes a holistic view of what constitutes DR and BC

The common view of DR/BC is that it involves ensuring the IT systems are backed up and made available following any disaster. However, DR/BC involves more than just the IT systems, and IBM provides a range of services that cover everything from buildings to the business. Ovum particularly likes the templates IBM has developed to help guide its customers through the maze of setting up the correct DR/BC plan for the organization.

Uses advanced analytics to help organizations understand the level of protection they have

IBM with its advanced analytics provides reporting and insights into the performance and coverage of any data protection plan. This insight helps organizations understand how effective any data protection plan is in terms of meeting customer expectations and the cost.

DRaaS provides a simple way to confirm any DR protection plan will operate when needed

IBM in its DRaaS service provides a simple way for any organization to test any DR plan and be confident that should it be needed it will deliver what was planned. The other key strength is that IBM's services include and encourage customers to carry out simulated disasters so that any processes are also tested. These simulations can be performed while the live systems are operating, which reduces the impact on the business and saves on IT costs, avoiding the typical weekend DR testing approach that requires business operations to be paused and IT to work all weekend to set up, test, and restore production systems.

IBM has more than 300 global data centers

The ability to hold any backup or DR data locally is important for data sovereignty reasons as well as performance. IBM has more than 300 data centers globally and can therefore be local in more markets.

Weaknesses

Cannot easily back up containers

IBM is in line with the rest of the market when it comes to the capability to back up and restore container (Docker) solutions. While IBM is more advanced than most in that it can back up and restore containers, it is not a simple or straightforward process.

Opportunities

To build more comprehensive analytics capabilities

IBM has one major advantage over its competitors: its IBM Watson technology. Ovum believes that by making greater use of cognitive computing and analytics, IBM services could enable organizations to understand their environment better and therefore develop better data protection plans.

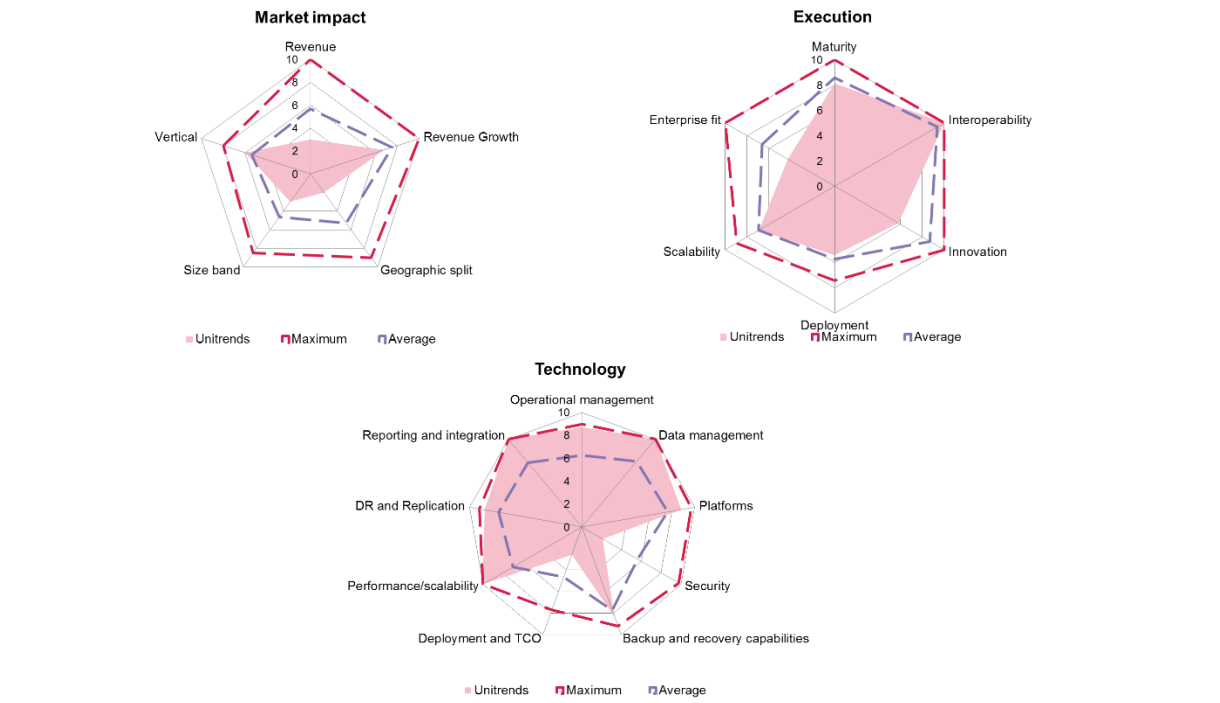
Threats

The nature of disasters changes so a wider area becomes affected

The idea that data can be protected and stored according to local data sovereignty laws is a strength of IBM with its 300 or so data centers, but this is also a threat if the area affected by a disaster means that local solutions become a part of the disaster area.

Unitrends (Ovum recommendation: challenger)

Figure 16: Unitrends radar diagrams



Source: Ovum

Products assessed in ODM

Connected Continuity Platform with Unitrends Enterprise Backup, Unitrends Cloud and Recovery Series appliance v9.0

ODM assessment

Unitrends delivered a mixed performance and narrowly missed out on being classified as a leader. In terms of market impact, Unitrends scored in line with the average in two of the five sub-categories. In the execution category, it recorded four out six sub-categories in line or above the average, and was particularly strong in interoperability where it was one of the leaders. Unitrends was also very strong in the technology category, with leading scores in six of the nine sub-categories (performance and scalability, DR and replication, reporting and integration, operational management, data management, and platforms), and one sub-category in line with the average, and two below-average sub-categories.

Ovum SWOT Assessment

Strengths

Provides a recovery guarantee

The automated backup and DR testing capability using certified recovery points enables Unitrends to guarantee that the data can be recovered to the correct point in time. This guarantee is something that most organizations either do not have or have to perform manual testing to verify. Unitrends with its automated approach reduces both the cost and human error in the verification process.

Protects all the data irrespective of where the data is stored

Unitrends has the concept of a single pane of glass, where it has visibility of all the data assets of an organization irrespective of where the data is stored. Unitrends believes the backup provider should not force an organization to adapt its environment to fit the tool, or worse, force it to use multiple tools to protect all of the IT assets. Unitrends supports virtual environments from VMware, Microsoft Hyper-V, and Citrix XenServer. It also supports a wide range of physical and guest operating systems including many versions of Windows, Linux, and legacy Unix-based systems, with common enterprise applications such as Microsoft Exchange, SQL Server, SharePoint, and Oracle DB natively supported.

Weaknesses

No specific containers capability currently

The lack of a specific capability to protect and restore containers technology (microservices) is common because the use of this new technology is not yet widespread and is handled by the containers vendor in a basic form. However, Ovum considers that 2016/17 will see the number of container solutions, and therefore the number of containers, increase to the point that specific protection solutions will be needed.

Opportunities

To build integration points with key new organizations developing DevOps solutions

While Unitrends is not a DevOps solution, its approach and technology can be integrated into agile development processes and tools. Ovum believes that Unitrends should consider licensing its technology to these specialist vendors, while also maintaining it messaging on its wider application. However, Unitrends does provide a REST API for third parties and partners to build custom solutions using its technology.

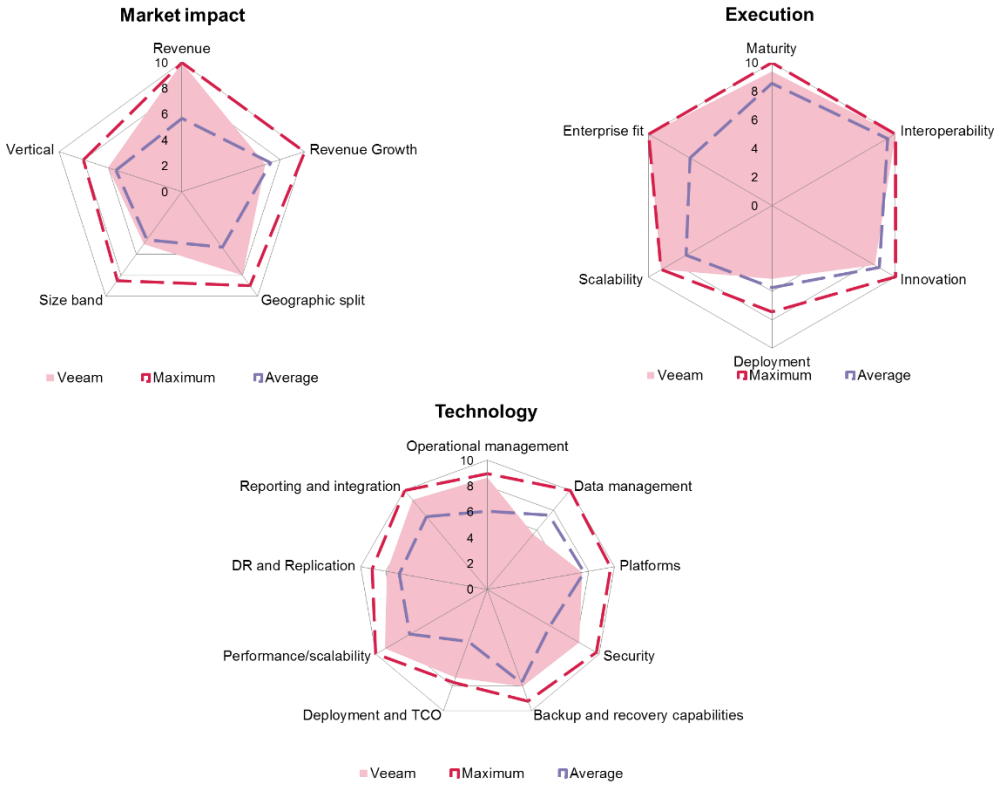
Threats

Cloud storage removes the enterprise customer from the equation

The whole concept of data protection and availability could become redundant for cloud providers as more and more organizations adopt a cloud-first strategy. In this scenario, enterprise customers would not invest in data protection and availability solutions, and would instead expect these services to be provided by the cloud provider. Ovum believes that this is not a very likely result of the move to cloud, but as cloud providers look to differentiate themselves, offering data protection services will become a reality, and this could provide an opportunity for Unitrends.

Veeam (Ovum recommendation: leader)

Figure 17: Veeam radar diagrams



Source: Ovum

Products assessed in ODM

Veeam Availability Suite v9.5

ODM assessment

Veeam has grown rapidly over the past couple of years, moving from being a challenger in 2014/15 to being the clear leader in 2016/17. In terms of market impact, Veeam is the category leader and all five sub-categories were in line or above the average, with leading scores for geographic split and revenue. Veeam performed well in the execution category where it was second overall and recorded all six sub-category scores in line or above the average, with sub-category leading scores for scalability, enterprise fit, maturity, and interoperability. In the technology category, Veeam was a leader with an average score of almost 8/10, and in line or above average for eight of the nine sub-categories. Ovum considers Veeam's performance to be particularly strong in terms of operational management, security, backup and recovery, performance and scalability, and reporting and integration.

Ovum SWOT Assessment

Strengths

Provides backup and replication in a single solution

Veeam Availability Suite embraces the philosophy that any backup strategy should include a disaster recovery and replication aspect. This approach enables any backup image to be used for a full system

recovery or the retrieval of an individual file, and it also allows for VMs to be replicated to a DR site for instant failover in the event of a disaster. The other advantage of a combined virtualized backup and replication solution is that organizations can run a VM from a backup file and therefore more quickly perform a full recovery from backup than when using traditional methods, and replication allows for VMs to be synchronized much more frequently with the DR site. Veeam is also expanding its portfolio to include agent-based technologies for Windows and Linux server instances, either in the cloud or on-premise, which rounds out its solution for to cover virtual, physical, and cloud-based workloads.

Native integration with the leading storage vendor's solutions

While native integration is not needed to protect data, it does provide Veeam with a very efficient way to make snapshots. By using the hardware capabilities, it removes the overhead on the hypervisor and therefore improves data protection efficiency.

Flexible licensing model

Veeam offers flexibility to license on a capex or opex model, or a combination of both. Veeam has also structured its licensing for service providers to align with the methods they use to bill customers, which in addition to perpetual licenses includes rental licenses on a per-VM-basis. For most customers this licensing flexibility offers a reduction in terms of licensing costs.

Provides automated testing of any DR or data protection plan

Veeam's virtual lab solution enables any data protection plan to be tested automatically to provide auditable evidence that the plan is verified. Ovum also likes the self-documenting capability of the plan based on Microsoft Word templates.

Weaknesses

Does not protect all the data associated with containers

Veeam has no comprehensive container protection solution, but it does protect the data lakes behind the containers. This is in line with other vendor solutions.

Opportunities

To develop more application specific solutions

The growth of online application suites such as Microsoft Office 365 have created a gap in the data protection market where not all the vendors support all the leading applications. Veeam, however, will offer a new product, Veeam Backup for Microsoft Office 365, in late 2016. Ovum believes that providing point solutions to protect the leading application suites is a good way to provide new customers with an on ramp for Veeam's wider data protection capabilities.

Threats

It becomes difficult to maintain quality across the partner ecosystem

Veeam has grown significantly over recent years, and recently surpassed the 200,000 customer mark. This impressive growth has been achieved through a channel-only strategy and Veeam has more than 41,000 channel partners globally. Ovum believes that as the ecosystem expands, the challenge of maintaining quality of service and support becomes harder. Veeam has recently introduced a tier partner program designed to match the partner level with the support and rewards received.

Vendor solution selection

Inclusion criteria

The 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 mixture of technologies, although x86 is the dominant technology in use and therefore any solution must operate in the x86 market. It must be noted that EMC, ExaGrid, NetApp, and Veritas declined to take part in this edition of the Ovum Decision Matrix.

The criteria for inclusion of a vendor in the Ovum Decision Matrix for data availability and protection in the cloud era 2016–17 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 be a mixture of midsize enterprises 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 consumer 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 from 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 Ovum Decision Matrix for Data availability and protection 2016–17 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 develop 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. The capability 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 five 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.
- Vertical penetration: Ovum determines each solution’s revenues in the following verticals: energy and utilities; financial services; healthcare; life sciences; manufacturing; media and entertainment; professional services; public sector; retail; wholesale and distribution; telecommunications; and travel, transportation, logistics, and hospitality. These revenues are calculated as a percentage of the market leader's revenues in each vertical, multiplied by 10, and then rounded to the nearest integer. The solution’s overall vertical penetration 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

Author

Roy Illsley, Principal 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

CONTACT US

www.ovum.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo