G00279272

Critical Capabilities for Enterprise Endpoint Backup

Published: 12 November 2015

Analyst(s): Pushan Rinnen, Robert Rhame

Endpoint backup has gone beyond simple backup/restore to a broader end-user data protection solution reducing various risks and increasing user productivity. This research helps I&O leaders evaluate enterprise endpoint backup solutions in two scenarios: cloud deployment and on-premises deployment.

Key Findings

- Endpoint backup is no longer a tactical product providing laptop file or device data recovery; IT leaders are looking for a more strategic solution to centrally manage user data that is typically unmanaged today.
- Product capabilities specific to laptop user file backup and restore are becoming increasingly similar, with the key differentiation being on capabilities to support frequent backup and more security features.
- Other key differentiations focus on protecting user data created on mobile devices or in the cloud, PC migration, and built-in compliance and e-discovery capabilities.
- The vast majority of the products are offered as a software as a service (SaaS) solution.

Recommendations

- Make full use of product capabilities when possible, including PC migration, mobile device support, remote wipe and compliance functions.
- For organizations using public cloud applications, such as Google Drive and Microsoft OneDrive, select products that offer a centralized protection and management platform for end-user data on local devices as well as in the cloud.
- For organizations with legal hold and e-discovery requirements, work closely with the internal legal and compliance team when making a product selection to ensure that important requirements are met.

What You Need to Know

Endpoint backup is fundamentally different from server backup. While server backup is mandatory to protect mission-critical data on servers with predictable operation schedules, endpoint backup deals with unmanaged data generated by users with unpredictable schedules and locations. With device proliferation and more user data residing in the cloud, endpoint backup is gradually morphing from a simple PC backup focus into a more comprehensive, end-user data protection and management platform — a foundation to build centralized and consistent policies to manage and govern end-user data no matter where it is located (on endpoint devices or in the cloud). Vendors are developing native capabilities or API plug-ins to provide e-discovery and compliance governance, as well as business analytics.

The industry has gone beyond the debate about whether enterprise file sync and share (EFSS) can replace endpoint backup (the answer is still "no," mainly due to security reasons). In fact, some vendors are developing capabilities to back up cloud EFSS applications at customers' requests.

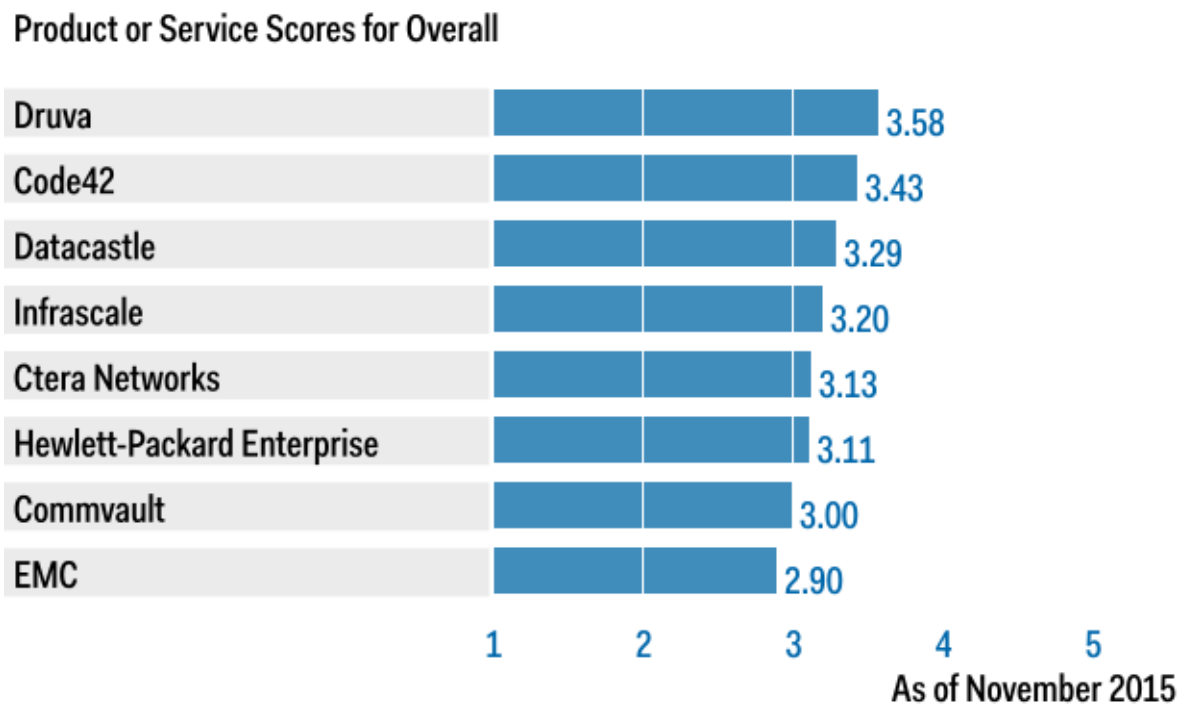
From the user perspective, all products evaluated in this research received high satisfaction scores from 62 customer references on user file backup and data retention upon employee departure. Other functions such as PC migration (focusing on personal settings, not just user files), remote wipe and data governance showed greater variation in scores, as some products have no or limited capabilities in those areas. References cited higher satisfaction with Windows PC backup than with Mac backup, with few applying the solution to mobile devices.

I&O leaders who worry about security because of unpredictable human behavior should adopt endpoint backup solutions to augment other security products and handle data loss risks.

Analysis

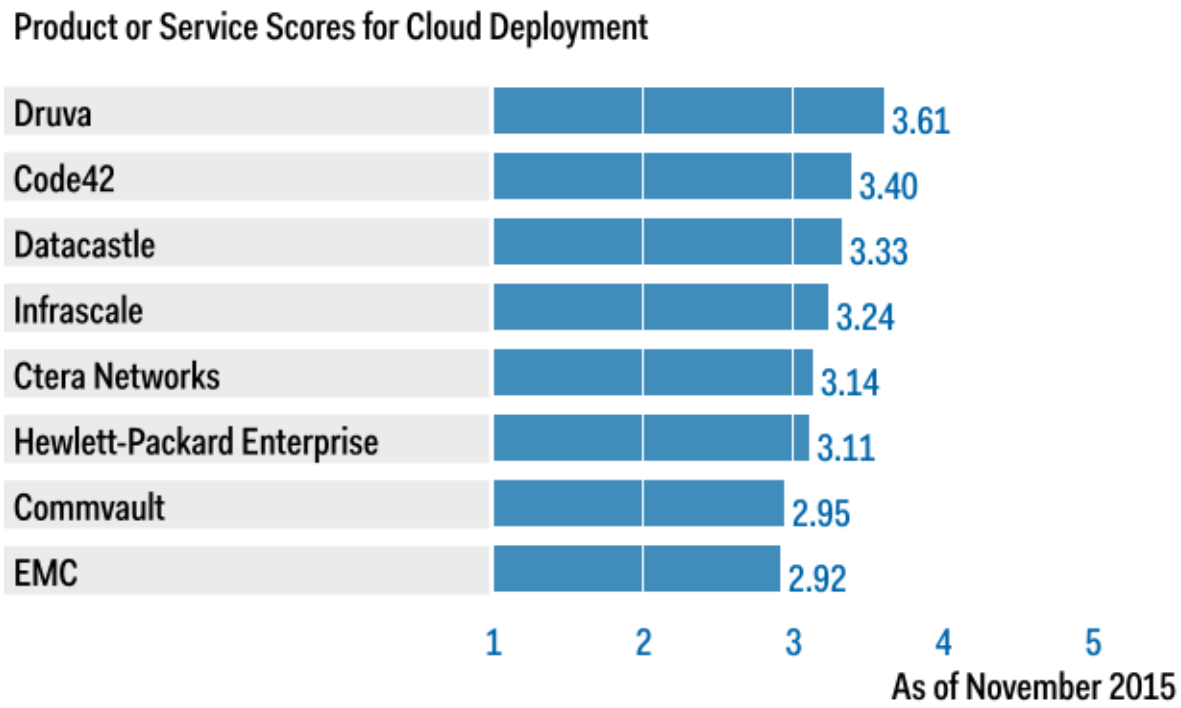
Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for Overall Use Case



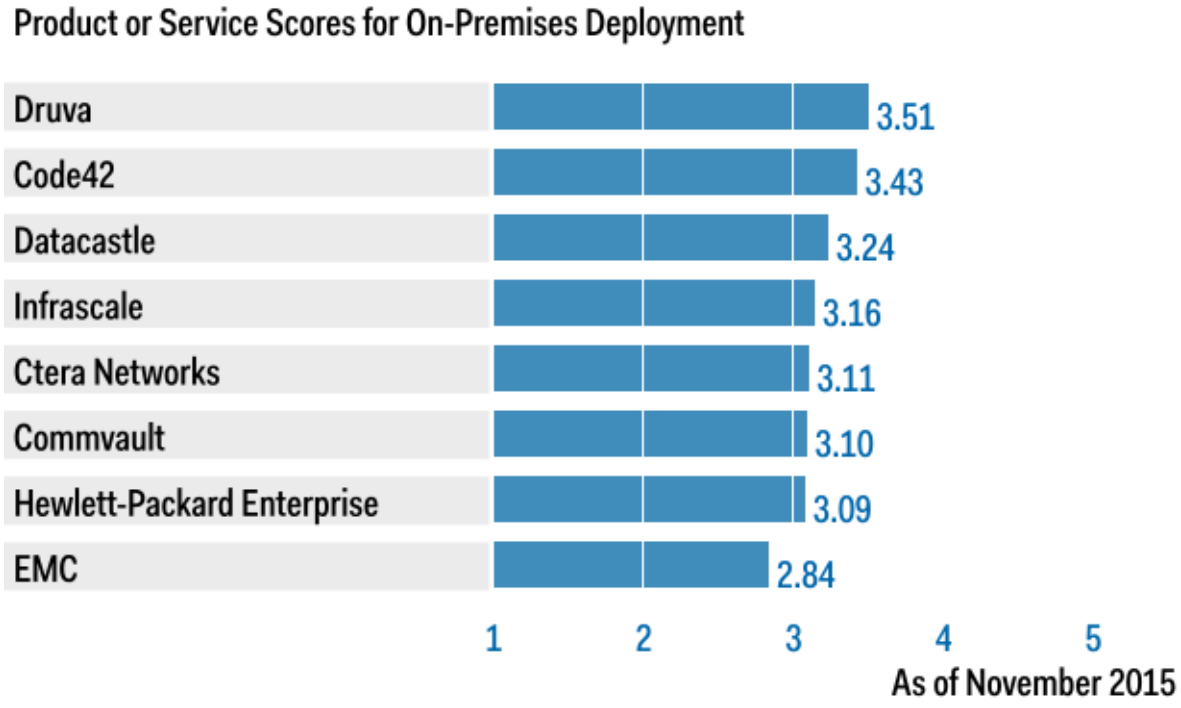
Source: Gartner (November 2015)

Figure 2. Vendors' Product Scores for Cloud Deployment Use Case



Source: Gartner (November 2015)

Figure 3. Vendors' Product Scores for On-Premises Deployment Use Case



Source: Gartner (November 2015)

Vendors

Code42

Code42 is one of the fastest-growing and leading enterprise endpoint backup vendors. While many large enterprise customers in the past have used the technology on their premises, new enterprise customers are increasingly adopting Code42's hybrid cloud deployment model where the encryption keys are stored on-premises and some or all backup data is stored in Code42's seven global data centers. The company's public cloud backup offering is primarily used by consumers and small and midsize businesses (SMBs). Code42's product, CrashPlan, appeals to enterprises that desire field-proven, scalable endpoint backup with frequent backup schedules and on-premises or hybrid cloud deployment models. Code42 has discontinued its EFSS solution in favor of ongoing development of e-discovery capabilities and backup capabilities for established popular cloud EFSS solutions. Weak areas include the limited use case of PC migration and mobile device support.

Commvault

Commvault is best known for its enterprise server backup. A small percentage of its customers use Commvault Endpoint Data Protection (CEDP) today, although many of them have deployed it on thousands of laptops and desktops. CEDP shares the same data repository as its server backup, allowing its Web console and mobile app to be able to download user files from laptop backup as well as file server and Exchange backup. It also leverages its native legal hold and e-discovery capabilities to protect endpoint data. The product supports a file modification option to enable backups to occur in a near continuous mode and only when there is changed data. The GUI has a useful preview feature before restore. On the down side, CEDP has weak public cloud (non-MSP) integration. Most customers have low backup frequency (long RPOs) and don't use CEDP for PC migration. Administrative experience is relatively more complex.

Ctera Networks

Ctera is a privately held company founded in 2008. The Ctera endpoint backup and EFSS products share a common architecture, and users of both do not require additional storage space. Customers may opt for a private cloud managed by its Web portal or have the flexibility to select from the wide range of supported public cloud deployments in an open or virtual private cloud deployment. Ctera's gateway appliance may be used for fast local restores and for remote locations with poor network connectivity. Ctera features client-side, block-level incremental forever backup with global deduplication and compression for storage and bandwidth reduction. The solution is missing federated search, full-text index and legal hold, and has very limited remote wipe capability for mobile devices only. While two-factor authentication is not available, Ctera does have the capability to restrict administrator login by IP address.

Datacastle

Datacastle offers backup software technology for managed service providers and does not provide its own BaaS services. Its largest service provider partner supports hundreds of thousands of devices in a single vault. Microsoft has been a key Datacastle partner and offers select large Azure customers a first-year free endpoint backup service promotion. Many other global IT service providers have adopted Datacastle technologies due to strong capabilities that are desired by service providers, such as the patented ability to encrypt data blocks before they are deduplicated; a centrally managed, encrypted local cache to speed up backup performance and secure global deduplication with multitenancy for more efficient backup storage. Endpoint backup services based on the Datacastle's solution appeal to organizations that desire frequent backup schedules, strong roaming detection and remote wipe capabilities. However, it is rarely deployed on-premises and is rarely used for PC migration. It lacks functions related to e-discovery and compliance governance.

Druva

Druva has been growing fast since 2010, when it launched its inSync endpoint backup software and online services using AWS native database and infrastructure. Unlike its competitors, which often started out with a consumer focus, Druva focuses entirely on midsize to large enterprise customers, the vast majority of which use the cloud deployment model. Druva has been aiming to go beyond simple backup by offering an integrated end-user data protection and management solution. The company was early to market with a unified platform for endpoint backup, sync and share, mobile support, and data loss prevention (DLP). It has since added more compliance and governance and analytics capabilities, as well as backup capabilities for cloud file sync and share applications. More recently, Druva added support for Azure global data centers as backup storage destinations to expand its global presence. It should be noted that although inSync allows customers to back up as frequently as every five minutes, most customers use the default four-hour or less frequent settings, which could result in undesirable data loss windows.

EMC

Mozy is part of EMC's Data Protection Suite and is primarily positioned for customers who want traditional cloud BaaS. Mozy guarantees same-day support for new OS releases from Microsoft and Apple. Mozy offers an idle system sensing function that enables it to perform frequent backups throughout the day, although Mozy does not support continuous data protection (CDP) or near CDP. The Mozy sync functionality is bundled at no additional cost and allows users to synchronize files between their own devices. Mozy has broad support for single sign-on providers, multiple attribute access validation capabilities, and an IP whitelist, but still no integration for two-factor authentication. Mozy does not offer advanced functions such as remote wipe, PC migration and data governance. Back-end cloud storage options are limited to EMC data centers in the U.S. and Europe with no cross-geographical redundancy.

Hewlett-Packard Enterprise

Hewlett-Packard Enterprise (HPE) introduced in the 2015 Connected MX PC backup, a new design from its traditional Connected product. The MX solution is available either online or hosted in HPE's cloud. It has delivered numerous features to close long-standing gaps that exist between

Connected and competitors, including CDP, global deduplication, a unified engine, and UI for backup and sync and share. Connected MX's mobile app allows content preview before download/restore. Still-missing features include a lack of mobile device backup capabilities, remote wipe, and limited backup throttling. Of particular concern for the SaaS solution, HP manages encryption keys in their data centers, and there is currently no other option. On the data governance side, there is no native full-text index/search, nor an embedded governance dashboard. Those functions are only available through its integration with Autonomy's Intelligent Data Operating Layer, a full-fledged large enterprise archiving and analytical platform with conceptual understanding of information. As the Connected MX product is fairly new, no references surveyed for this research have used the CDP function.

Infrascale

Infrascale started out as a PC backup technology and service provider targeting consumers and SMBs. Today, it offers an integrated server/endpoint backup and disaster recovery as a service solution for small and midsize enterprises. Its largest endpoint backup customer supports 45,000 devices, and several MSP partners back up over 100,000 devices. Infrascale has a comprehensive feature set and a single-client agent for both endpoint backup and file sync and share. Customers that purchase the Cloud Failover Appliance receive endpoint backup free of charge. For a small vendor, it has surprisingly wide geographic coverage for its cloud service offering, including Brazil and South Africa. Infrascale's technology can be used in a private cloud or a public cloud IaaS environment. Although backup can be scheduled as frequently as every 15 minutes with a near CDP option, many references schedule backup only once a day with 24-hour data loss windows. Some of Infrascale's references are relatively small, and the product lacks data governance functions.

Context

Endpoint backup is evolving from a device-centric approach to user-data-centric protection and management platforms. Public cloud and hybrid cloud deployments have gone up significantly in the past two years. As a result, vendor development has recently been focusing on how to provide a centralized data management tool to manage end-user data no matter where it resides (on a local device or in the cloud). What's more, governance, compliance and e-discovery functions are being added natively or through third-party ISVs via API integration. In this expanded use case, endpoint backup becomes a central repository and data source to more intelligently manage unstructured data generated by end users. Such data has typically been unmanaged but is becoming more prolific.

Product/Service Class Definition

Enterprise endpoint backup refers to backup of endpoint devices, such as desktops, laptops, tablets and smartphones, which can access corporate content and create business content locally. There are numerous PC backup products in the market, especially for consumers and small businesses. The focus of this report is on the products that have a proven ability to meet enterprise endpoint backup support and implementation requirements.

Critical Capabilities Definition

Client Diversity

This capability measures the degree of diversity in PC OS platforms, the timeliness to support the new version of the key PC OS platforms and, to a lesser degree, the capability to back up user files created directly in the cloud, such as Google Drive and Microsoft OneDrive.

PC Migration

PC migration, although not a key traditional backup capability, has become very useful to help reduce user downtime and increase user productivity. This capability measures the ability to migrate the entire PC content to a new device, including system and personal settings.

Mobile Device Support

This capability measures the mobile app's functions to access and download backup files, as well as to back up data generated by mobile apps such as camera and contacts. It measures the ability to avoid backup traffic on cellular networks and the ability to support EFSS.

Performance

This capability evaluates the techniques to boost backup and restore performance, such as backup methods, deduplication and local cache, as well as network, disk I/O and CPU throttling. Offline shipping for initial seeding and restore of large datasets are also measured.

Backup Frequency

This function, also known as recovery point objective (RPO), measures how a data loss window can be reduced by more frequent backup, especially for the mobile workforce. We look at the default schedule, the most frequent schedule supported and customer references' schedules.

Scalability

This capability measures the size of the deployments in the real world, such as the largest deployment in production and the references' deployment sizes, as well as any limitations for file size and count.

Security

This capability evaluates functions such as cloud security, encryption and industry standards certification, access control methods, and remote wipe/remote tracking.

User/Administrator Experience

This capability examines end-user experiences such as self-service restore and administrative functions such as delegation, updates, monitoring/reporting and user interface ease of use.

Public Cloud Integration

This capability evaluates the product's integration with public cloud, supported by evidence of overall endpoint backup business generated via cloud services and the breadth of the geographic coverage in terms of data center locations used by a single-service provider.

Resiliency and Storage Efficiency

This capability measures the infrastructure functions significant to on-premises deployments, including server/storage high availability, data integrity checks and storage efficiency techniques.

Data Governance

This capability examines functions that allow organizations to manage data governance such as full-text search, in-place legal hold, audit trail, and integration capabilities with e-discovery tools.

Use Cases

Overall

Each product capability for the overall scores is weighted and balanced based on the significance for the majority of the users.

Overall use case is a generalized usage scenario. It does not represent the ways specific users will utilize or deploy technologies or services in their enterprises.

Cloud Deployment

Each product capability for the overall scores is weighted against the needs when deploying the solution in the cloud.

Cloud deployments carry more weight in capabilities such as proven cloud presence and security. Both cloud and on-premises deployments share the same weighting on several critical capabilities such as client diversity, mobile support, performance, backup frequency and e-discovery functions, as users typically have the same requirements regardless of whether the solution is deployed in the cloud or on-premises.

On-Premises Deployment

Each product capability for the overall scores is weighted against the needs when deploying the solution on-premises.

On-premises deployments carry more weight in capabilities such as scalability, infrastructure resiliency and storage efficiency, as well as administrative experiences because internal IT has to manage the backup infrastructure. Both cloud and on-premises deployments share the same weighting on several critical capabilities such as client diversity, mobile support, performance,

backup frequency and e-discovery functions, as users typically have the same requirements regardless of whether the solution is deployed in the cloud or on-premises.

Vendors Added and Dropped

Added

Two vendors are added this year: Ctera Networks and Infrascale.

Dropped

Asigra was dropped this year due to its failure to meet the new market presence criterion.

Inclusion Criteria

The inclusion criteria for various endpoint backup products focus on enterprise-level support with proven field installations for midsize and large enterprises.

- The product must, at minimum, be able to back up the latest Windows operating system for PCs.
- The product targets midsize to large enterprise customers with a centralized common management tool.
- The product is developed and owned by the vendor. If the product is sourced from an OEM partner, it is not qualified for separate evaluation.
- The vendor must:
  - Either generate $10 million or more in revenue specifically from endpoint backup sales from 1 July 2014 to 30 June 2015
  - Or, alternatively, the product currently backs up 100,000 or more endpoint devices for enterprises with at least 500 employees
- The vendor must provide at least five production reference customers.
- The vendor or its OEM partners have their own cloud data centers or leverage public cloud partner data centers in at least two major geographies (such as North America, Latin America, Europe/Africa and Asia).

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Overall	Cloud Deployment	On-Premises Deployment
Client Diversity	8%	8%	8%
Mobile Device Support	5%	5%	5%
PC Migration	7%	7%	7%
Performance	15%	15%	15%
Backup Frequency	15%	15%	15%
Scalability	9%	6%	12%
Security	7%	8%	6%
User/Administrator Experience	10%	8%	12%
Public Cloud Integration	10%	15%	0%
Resiliency and Storage Efficiency	6%	5%	12%
Data Governance	8%	8%	8%
Total	**100%**	**100%**	**100%**
			As of November 2015

Source: Gartner (November 2015)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2. Product/Service Rating on Critical Capabilities

Critical Capabilities	Code42	Commvault	Ctera Networks	Datacastle	Druva	EMC	Hewlett-Packard Enterprise	Infrascale
Client Diversity	3.4	3.1	3.2	3.2	3.2	3.2	2.8	3.2
Mobile Device Support	2.1	3.2	2.0	2.9	3.7	2.5	3.3	3.1
PC Migration	3.0	2.2	3.0	1.1	3.4	1.1	1.7	2.8
Performance	3.8	3.2	3.7	4.0	3.5	3.1	3.4	3.6
Backup Frequency	4.0	3.1	3.2	3.9	3.1	3.3	3.1	3.1
Scalability	4.3	3.3	3.6	3.3	3.7	3.7	3.9	3.2
Security	3.0	2.8	3.1	3.5	3.9	3.1	2.3	3.6
User/Administrator Experience	3.6	3.1	3.1	2.9	3.6	2.9	3.3	3.1
Public Cloud Integration	3.5	2.3	3.6	4.0	4.3	3.8	3.8	3.8
Resiliency and Storage Efficiency	3.1	3.2	3.4	3.7	3.6	3.0	3.4	3.5
Data Governance	2.2	3.4	1.4	2.2	3.7	1.0	2.5	1.9
								As of November 2015

Source: Gartner (November 2015)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product Score in Use Cases

Use Cases	Code42	Commvault	Ctera Networks	Datacastle	Druva	EMC	Hewlett-Packard Enterprise	Infrascale
Overall	3.43	3.00	3.13	3.29	3.58	2.90	3.11	3.20
Cloud Deployment	3.40	2.95	3.14	3.33	3.61	2.92	3.11	3.24
On-Premises Deployment	3.43	3.10	3.11	3.24	3.51	2.84	3.09	3.16
As of November 2015								

Source: Gartner (November 2015)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"How to Address Three Key Challenges When Considering Endpoint Backup"

"How to Leverage Public Cloud IaaS for Backup"

"Hype Cycle for Storage Technologies, 2015"

"How Products and Services Are Evaluated in Gartner Critical Capabilities"

"Magic Quadrant for Enterprise Backup Software and Integrated Appliances"

Evidence

This research uses multiple data sources including user inquiries, one-on-one vendor meetings, vendor surveys and customer reference online surveys.

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp