Critical Capabilities for Enterprise Endpoint Backup

9 October 2012 ID:G00235971

Analyst(s): Pushan Rinnen, Dave Russell, Alan Dayley

VIEW SUMMARY

This document provides detailed stack ranking of 11 endpoint backup products against 12 critical capabilities and across two use cases. Users can use this research to narrow down their enterprise endpoint backup product shortlist.

Overview

Key Findings

- Backup vendors that offer strong server backup solutions often lag behind endpoint-focused providers with their endpoint backup solutions.
- With the exception of Copiun, all top-rated endpoint backup products support backup to their own cloud or to third-party cloud infrastructure.
- Most products offer solid laptop backup support, yet many are ill-equipped to support the upcoming bring your own device (BYOD) scenario due to their lack of integration with security products that offer separation of corporate content from personal content.
- While all products evaluated in this research have good capabilities in encryption and user-transparent agent deployment and backup, there are still a lot of variances in their capabilities to support cloud-oriented functions (such as file sync/share), e-discovery, and the integration with data loss prevention (DLP) features, such as remote wipe and remote tracking.

Recommendations

- Work closely with the endpoint security/compliance team, the mobile team, and human resources to design a comprehensive corporate plan for endpoint protection, including backup.
- Choose endpoint backup products based on employees' risk profiles. The mobile workforce tends to be more at risk than office workers and will need a product that has more built-in security features, more data capture capabilities and better self-service experiences.
- Continue to evaluate products in the endpoint backup space as technologies and solutions are fast-changing.

What You Need to Know

Endpoint backup today is a practice mostly applied to desktops and laptops, although it will be changing very fast in the next few years to incorporate tablets and smartphones. Until recently, endpoint backup has often been neglected by many organizations, as well as by backup software vendors, which tend to focus on server backup.

The emergence of iPads and other tablets, especially the increasing business use of those devices, which are at the forefront of the BYOD trend, has made endpoint protection, including backup, a hot topic. This research has found a significant gap between what users need and what vendors offer regarding tablet and smartphone protection. Among the 11 endpoint backup products we evaluate and profile in this report, two products have only limited backup capabilities for iOS and Android, although many do allow tablets and smartphones to access or download backed-up data.

Granted, the majority of business use cases of tablets and smartphones today are for email and content viewing. However, tablets are increasingly used as data creation and data modification tools. The lack of robust enterprise-level endpoint backup products from major vendors has driven many organizations to allow employees to use often consumer-grade file sync/share services, which could pose serious potential risk to businesses. It is encouraging to see that some endpoint backup vendors have also entered the file sync/share arena in an attempt to offer a more secure service to the enterprise. Over time, we believe enterprise endpoint backup needs to be an integral part of the overall endpoint protection solution, which should offer secure access, secure collaboration, secure

EVIDENCE

Gartner conducted a kiosk survey at the June Infrastructure & Operations Management Summit regarding endpoint backup. The results matched our findings from client inquiries and our overall observation that many organizations have no formalized policy and/or they depend on end users to find a method to protect endpoint devices. Among the 73 survey respondents, 27% and 39% let users find their own way to protect data on their laptops and tablets/smartphones, respectively. About 26% of respondents do not have a protection plan for their employees' tablets/smartphones but believe that such a policy is a priority.

NOTE 1
CRITICAL CAPABILITIES METHODOLOGY

"Critical capabilities" are attributes that differentiate products 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.

This methodology requires analysts to identify the critical capabilities for a class of products. Each capability is then weighted in terms of its relative importance overall, as well as for specific product use cases. Next, products 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 overall, and for each use case, is then calculated for each product.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor: most or all defined requirements not achieved

2 = Fair: some requirements not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

Product viability is distinct from the critical capability scores for each product. It is our assessment of the vendor's strategy and its ability to enhance and support a product over its expected life cycle; it is not an evaluation of the vendor as a whole. Four major areas are considered: strategy, support, execution and investment. Strategy includes how a vendor's strategy for a particular product fits in relation to its other product lines, its market direction and its business overall. Support includes the quality of technical and account support as well as customer experiences for that product. Execution considers a vendor's structure and processes for sales, marketing, pricing and deal management. Investment considers the vendor's financial health and the likelihood of the individual business unit responsible for a product to continue investing in it. Each product is rated on a 5-point scale from poor to outstanding for each of these four areas, and it is then assigned an overall product viability rating.

The critical capabilities Gartner has selected do not represent all capabilities for any product and,

backup and DLP.

This Critical Capabilities report is designed to compare the two common use cases — mobile-workforce-centric versus office-workforce-centric — against 12 critical capabilities. Among the 11 products we evaluate and profile in this report, we have found that a few relatively new products from startups and a few cloud backup technology providers are rated higher than the desktop/laptop modules from server backup vendors.

Return to Top

Analysis

Introduction

Endpoint backup is evolving to meet new challenges brought forth by new technologies, such as Apple's iPads and other tablets, and the new business practice of BYOD. Historically, endpoint backup has not been adopted as widely as server backup, which is regarded as more business-critical. Many organizations try to enforce a policy of asking users to write to network shares to avoid the complexity and the additional cost of backing up endpoint devices. Gartner believes that the increased mobility of the workforce and business adoption of tablets are forcing organizations to face the challenge of protecting and backing up the portable devices their employees use. As a result, we are receiving an increasing volume of user inquiries on endpoint backup. This Critical Capabilities report aims to help organizations evaluate 11 endpoint backup products in the market, both for on-premises and cloud deployments.

Return to Top

Product Class Definition

Endpoint backup refers to backup of endpoint devices, such as desktops, laptops, tablets and smartphones. There are numerous PC backup products in the market, especially for consumers and small businesses. This report focuses on the products we are aware of that have proved their enterprise endpoint backup support. For this report, Gartner defines endpoint devices as desktops, laptops, tablets and smartphones that can access corporate content and create business content locally.

Return to Top

Critical Capabilities Definition

All endpoint backup products profiled in this report share some basic feature functions, such as centralized management, user transparency in terms of both agent deployment and backup, backup of files and email archives, restore to a different device, and the support of scheduled backup and interrupted backup where backup jobs resume where they have stopped. This research focuses on the following 12 critical capabilities that differentiate competing endpoint backup products:

- Device/OS diversity: Degree of diversity in endpoint devices and endpoint OS platforms supported
- Content variety: Type of local content that can be backed up and restored
- Heterogeneous restore: Ability to restore to a different device and/or a different OS platform
- Scalability: Size of the deployment in the real world, not based on product design
- Performance: Performance-boosting techniques, such as incremental backup, compression, and throttling for network bandwidth and CPU cycles
- Data reduction techniques: Type of data reduction techniques, such as file-level single-instance restore, or block-level or object-level data deduplication
- Data capture frequency: How frequent the backup data can be captured
- Security: Commonly deployed security features, such as access control methods, encryption, and remote wipe and remote tracking of devices
- Administrator experience: Factors impacting administrator experiences, such as silent deployment of group or companywide policies, task delegation, separation of corporate content from personal content, reporting tools, and so forth
- User experience: Factors impacting user experiences, such as user interface, self-restore capability, single sign-on and whether there is a mobile app
- Cloud services support: Degree of supporting the vendor's own cloud or third-party cloud
- E-discovery functions: Functions that allow easy e-discovery for compliance, such as full-text indexing and search, federated search, and support of legal hold

Return to Top

Use Cases

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 an acquisition decision.

Since the use cases have to be supported by all products evaluated, we are rating the endpoint backup products for the following two use cases:

- Mobile-workforce-centric: With this use case, endpoint backup software needs to cater to the dynamic and unpredictable online/offline schedules of the mobile workforce, as well as the unsecure environment outside corporate firewalls. Among all critical capabilities, the flexibility of data capture choices, security features, user self-restore and cloud services support have high weighting for this use case.
- Office-workforce-centric: With this use case, endpoint backup software caters to a workforce that is always online during predictable business hours. These kinds of employees are typically sitting within a company's firewall (office workers) or connected via a secure corporate VPN (telecommuters). For this workforce, they need their endpoint backup to be nonintrusive and nondisruptive to their daily work. Therefore, silent deployment of backup agents, companywide policy-driven configurations, administrative experiences, performance and the variety of endpoint content that can be backed up are highly weighted critical capabilities for this use case.

Figure 1 looks at the weightings of all use cases in this research. Each use case weighs the capabilities individually based on the needs of that case, which impacts the score. Each vendor may have a different position based on its capability and the weighting for each one. The overall use case is the general scoring for the vendor's product, which is the average of the two different use cases.

Figure 1. Weighting for Critical Capabilities in Use Cases

Critical Product Capabilities	Overall	Mobile-Workforce-Centric	Office-Workforce-Centric
Device/OS Diversity	7.0%	8.0%	6.0%
Content Variety	10.0%	5.0%	15.0%
Heterogeneous Restore	2.5%	3.0%	2.0%
Scalability	8.0%	6.0%	10.0%
Performance	11.0%	7.0%	15.0%
Data Reduction Techniques	6.0%	6.0%	6.0%
Data Capture Frequency	10.5%	15.0%	6.0%
Security	10.0%	15.0%	5.0%
Administrator Experience	10.0%	5.0%	15.0%
User Experience	10.0%	15.0%	5.0%
Cloud Services Support	7.5%	10.0%	5.0%
E-Discovery Functions	7.5%	5.0%	10.0%
Total	100.0%	100.0%	100.0%

Source: Gartner (October 2012)

Return to Top

Inclusion Criteria

The inclusion criteria for various endpoint backup products focus on enterprise-level support with proven field records and a central management console.

Gartner invited Symantec and SOS Online Backup to participate in this evaluation, but both vendors declined.

The detailed inclusion criteria are listed as follows:

- In addition to desktop backup, the product must be able to support portable endpoint devices (at least laptops, with tablet and smartphone support as a plus).
- The product targets large-enterprise customers, as well as small or midsize businesses (SMBs), with basic enterprise-class capabilities, such as a centralized common management tool for multiple devices and the capability to support at least 1,000 endpoint devices.
- 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. For example, EVault, a Seagate company, offers an endpoint backup solution, but the product is not included because Datacastle is the technology's OEM.
- The product must have an installed base of at least 100 business customers (with at least 100 employees) or have at least 100,000 endpoint devices being managed.
- The vendor must be able to provide at least three reference customers who are using the product's key features.

Return to Top

Critical Capabilities Rating

Each of the products that meet our inclusion criteria has been evaluated on the critical capabilities, on a scale of 1.0 to 5.0 (see Note 1 for a discussion of our methodology):

- 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 and exceeds some requirements.
- 5 = Outstanding: Significantly exceeds requirements ("best in class").

For each of the capabilities, we assessed various aspects associated with that specific capability with ratings and established a baseline for Rating 3 (meeting requirements). The aggregate result of those aspect ratings represents the overall rating for that particular capability.

The baselines for each of the capabilities are described as follows:

- Device/OS diversity: Products that meet requirements can back up desktops and laptops and can download backup files to tablets/smartphones. They can also back up both Windows and Mac OSs. Those that can back up tablets and smartphones and those that support additional OS platforms receive higher ratings.
- Content variety: Products that can back up files and email archives are meeting requirements. Those that can back up additional content, such as contacts and personal settings, receive higher ratings.
- Heterogeneous restore: Products that can restore files to a different device or an OS are meeting requirements.
- Scalability: Products that meet requirements back up about 500 endpoint devices on average per enterprise customer. The largest deployment tends to be between 5,000 and 10,000 devices.
- Performance: Products that meet requirements support block-level incremental backup and source-side compression, as well as network and CPU throttling, with limited backup impact on CPU cycles. Those that offer additional performance-boosting techniques receive higher ratings.
- Data reduction techniques: Products that meet requirements support source-side single-instance store or deduplication. Those that offer target-side deduplication and global deduplication are exceeding expectations. Those that offer more efficient deduplication algorithms receive higher ratings.
- Data capture frequency: Products that meet requirements support near-continuous data protection, on-demand backup, scheduled backup and interrupted backup. Those that have smaller backup windows receive higher ratings.
- Security: Products that meet requirements support Active Directory, encryption for data in flight and at rest, and VPN-less backup over the Internet. Those that have more robust implementation techniques and more security features, such as single sign-on, remote wipe and remote tracking, receive higher ratings.
- Administrator experience: Products that meet requirements support a central management console and silent deployment of group of companywide backup policies. They can delegate their tasks and have reporting tools that show backup frequency and success rates. Those that support a more intuitive graphical interface or bare-metal restore (BMR) receive higher scores.
- User experience: Products that meet requirements have easily understood terms in the user interface, with easy navigation, and allow users to restore their own files. Those that have a more intuitive graphical interface or support full-text search or mobile apps receive higher scores.
- Cloud services support: Vendors with products that meet requirements have established their own cloud storage offering or a partnership with public cloud storage providers. They should have a reasonable percentage of customers using the cloud backup services. Additional services, such as file sync/share, result in higher ratings.
- E-discovery functions: Products that meet requirements offer flexible retention policies. Those that offer full-text indexing and search, federated search, and legal hold receive higher ratings.

Figure 2 shows the numeric ratings for each endpoint backup product.

Figure 2. Product Rating on Critical Capabilities

Product Rating	Asigra/Cloud Backup	Autonomy/Connected	CA/ARCserve	Code 42/CrashPlan	CommVault/Simpana DLO	Copiun/Copiun Data Manager	Datacastle/Red	Druva/inSync	EMC/Avamar Desktop/ Laptop	EMC/Mozy	IBM/TSM FastBack for Workstations and TSM Backup-Archive Client
Device/OS Diversity	3.7	3.0	2.5	3.4	3.4	3.4	3.2	3.7	2.5	3.0	2.2
Content Variety	3.6	3.5	3.4	3.7	3.6	3.4	3.0	3.6	3.1	3.2	3.2
Heterogeneous Restore	3.0	3.0	2.0	3.0	3.0	3.0	3.0	3.0	3.0	3.0	3.0
Scalability	4.0	4.5	2.0	3.5	3.8	4.0	2.5	3.5	3.0	3.0	3.0
Performance	3.0	2.6	3.0	3.7	3.3	3.8	3.2	3.4	2.8	3.0	3.3
Data Reduction Techniques	3.6	3.0	3.3	3.5	3.7	3.7	3.5	3.7	3.8	2.7	3.3
Data Capture Frequency	3.0	2.5	2.6	3.1	2.5	3.1	3.0	3.1	2.5	2.5	3.1
Security	3.1	3.3	2.6	3.1	3.1	3.4	3.3	3.3	2.6	2.7	3.0
Administrator Experience	3.4	3.0	2.8	3.6	3.0	3.6	2.9	3.7	3.2	2.7	2.6
User Experience	3.5	3.2	2.4	3.4	2.9	3.8	3.0	3.8	2.7	3.2	2.9
Cloud Services Support	3.6	4.1	2.1	4.1	1.9	1.9	3.0	3.3	2.7	4.4	1.9
E-Discovery Functions	3.1	3.5	2.8	3.3	3.5	3.5	3.0	3.4	3.0	2.8	3.0

Enlarge

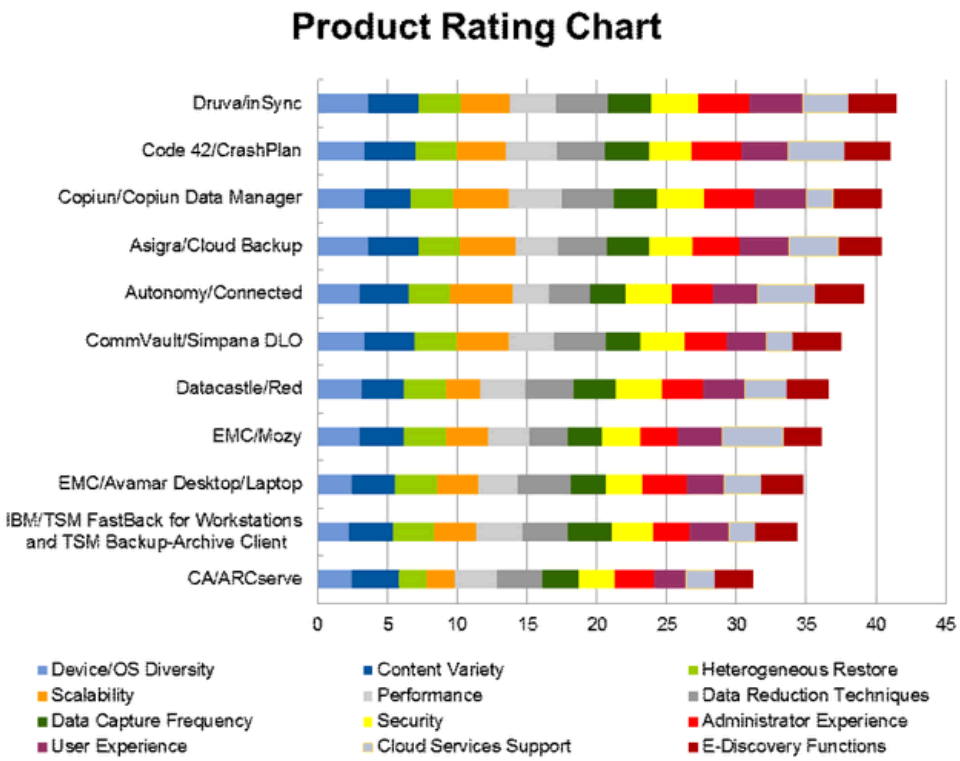
DLO = Desktop/Laptop Option
TSM = Tivoli Storage Manager

Source: Gartner (October 2012)

Return to Top

To determine an overall score for each product in the use cases, the ratings in Figure 2 are multiplied by the weightings shown in Figure 1. These scores are shown in Figure 3, which also provides our assessment of the viability of each product.

Figure 3. Product Rating Chart



Source: Gartner (October 2012)

Return to Top

Each product is rated on a 5-point scale from poor to outstanding for each of these four areas, and it is then assigned an overall product viability rating (see Figure 4). The weighted capabilities scores for all use cases are displayed as components of the overall score (see Figures 5, 6 and 7).

Figure 4. Product Viability Rating

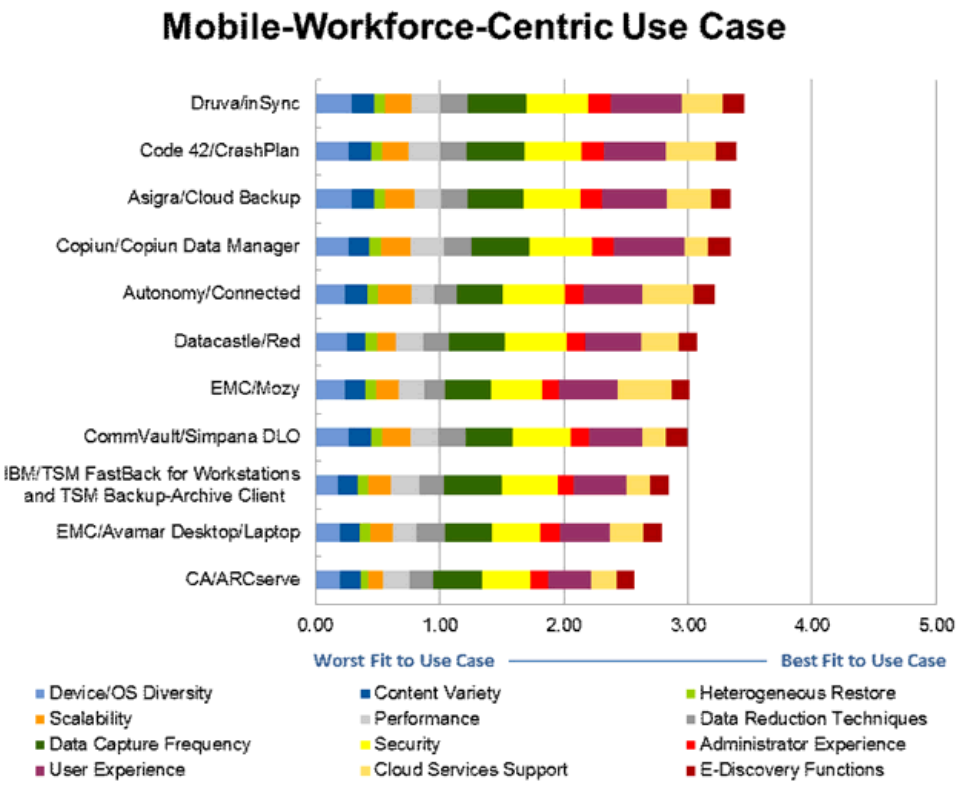
Vendor/Product Name	Asigra/Cloud Backup	Autonomy/Connected	CA/ARCserve	Code 42/CrashPlan	CommVault/Simpana DLO	Copiun/Copiun Data Manager	Datacastle/Red	Druva/inSync	EMC/Avamar Desktop/ Laptop	EMC/Mozy	IBM/TSM FastBack for Workstations and TSM Backup-Archive Client
Product Viability	Good	Good	Fair	Excellent	Good	Good	Good	Excellent	Good	Fair	Good

Enlarge

Source: Gartner (October 2012)

Return to Top

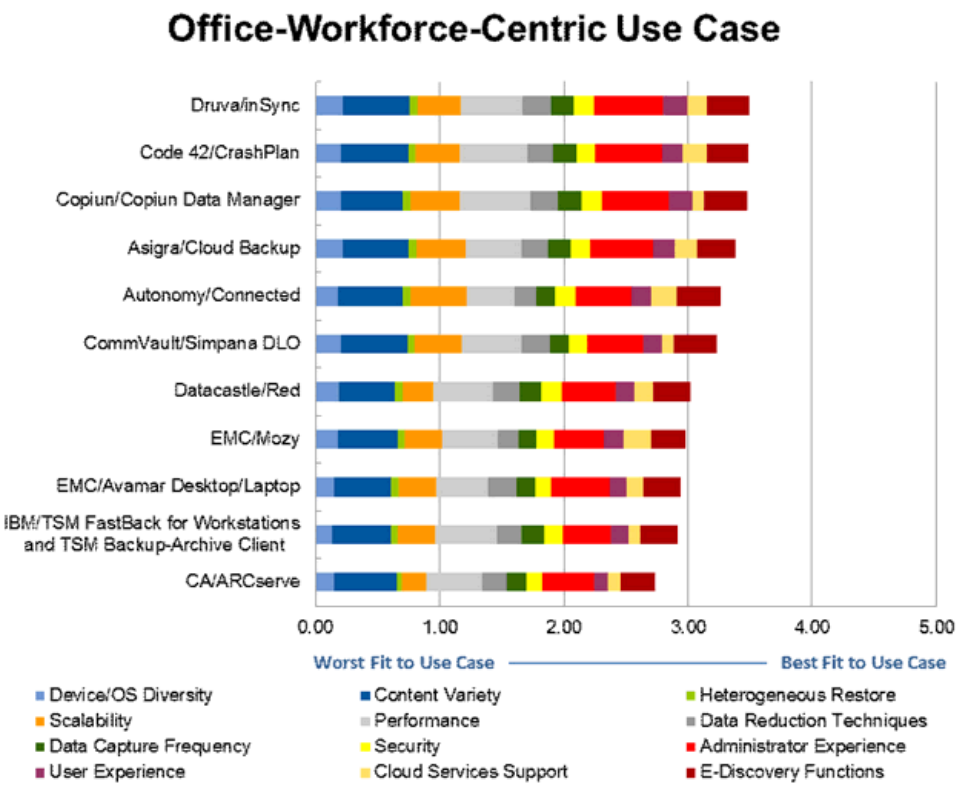
Figure 5. Product Rating Chart for the Mobile-Workforce-Centric Use Case



Source: Gartner (October 2012)

Return to Top

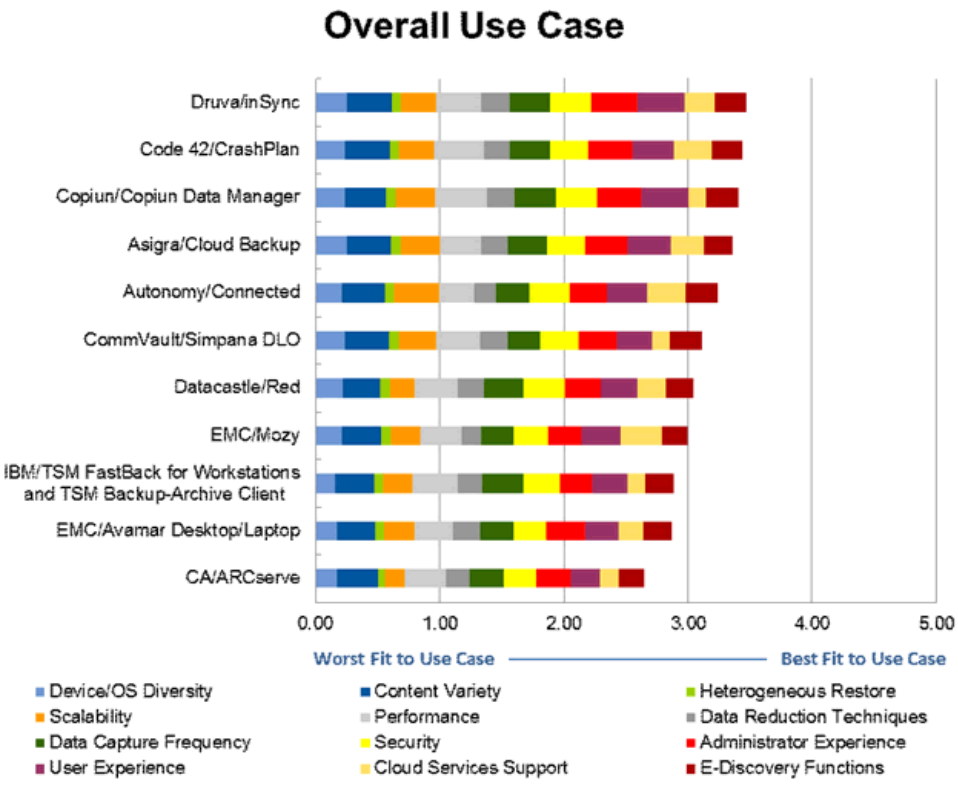
Figure 6. Product Rating Chart for the Office-Workforce-Centric Use Case



Source: Gartner (October 2012)

Return to Top

Figure 7. Product Rating Chart for the Overall Use Case



Source: Gartner (October 2012)

Return to Top

Vendors

Asigra

Asigra, a Toronto-based company, is known in the industry for its server and endpoint backup and recovery solutions designed for managed service providers, although some companies also use its product for private cloud implementation. The endpoint support of its Cloud Backup stands out in many areas, especially with its iOS and Android backup capabilities and support for capture of a variety of content associated with those mobile platforms. Its Cloud Backup is also scalable, with 50,000 endpoint devices as the largest deployment. The product supports source-side deduplication, as well as target-side global deduplication. User interface is graphical, with experiences similar to the device's native user interface. Asigra's Cloud Backup does not have native DLP features or DLP partners. It also lacks file sync/share and full-text index/search capabilities.

Return to Top

Autonomy, an HP Company

Autonomy acquired Iron Mountain's digital assets, including the online PC backup product and service Connected Backup, in May 2011. In October 2011, HP acquired Autonomy for more than $10 billion. Autonomy's Connected Backup is rated highly with scalability as it has 1,500 customers backing up 4 million endpoint devices. HP is the largest user, with 250,000 PCs being backed up to the Connected Cloud. The product is one of the very few in the market that supports full-text index/search and federated search through its integration with Autonomy's Intelligent Data Operating Layer, a common information platform for structured and unstructured information that provides conceptual understanding of information. Connected is also one of the data sources for Autonomy Legal Hold. However, Connected Backup does not offer more frequent data capture techniques, such as continuous data protection, and its source-side data reduction technique is based on the less granular file level.

Return to Top

CA Technologies

The support of endpoint backup is fairly new to CA Technologies' ARCserve Backup, which has established good presence for server backup in the SMB market. For endpoint backup, CA mostly promotes its image-based backup for Windows clients, with granular file recovery and BMR capabilities. ARCserve Backup has strong source-side deduplication and compression; it also supports global deduplication. Its cloud deployment supports only file backup, which has only target-side deduplication support. CA's endpoint backup product does not allow file restore to a different OS platform, and it has limited Microsoft Active Directory support. Compared with its peers, its real-world endpoint deployments have a smaller scale.

Return to Top

Code 42 Software

Code 42 is headquartered in Minneapolis. Founded in 2001, the company recently raised more than $55 million in private equity. CrashPlan, CrashPlan PRO and CrashPlan PROe are the respective names for its consumer, SMB and enterprise endpoint backup products (CrashPlan will be used as a generic name for all three throughout the rest of this document). Code 42 claims to have more than 5,000 business customers with more than 100 employees, with its largest deployment being 160,000. It manages 150PB of backup data in its global six data centers, backing up nearly 1 million endpoint devices. CrashPlan can be deployed either on-premises or as a hosted service, and users can even choose to split the backup stream and store on-premises and in the cloud using one backup job. CrashPlan supports Windows Mobile, Android and iOS for restore only. CrashPlan's interface has been cited by customers (both users and administrators) as being easy to use. Full-text search, remote wipe and BMR are not supported. Active Directory integration is supported, as is CPU, network and input/output throttling.

Return to Top

CommVault

CommVault is best-known for its Simpana enterprise server backup suite, with more than 16,000 customers. The company's Edge Data Protection offering is available stand-alone for endpoint backup or as part of an enterprise server backup solution. The largest reference customer has currently deployed the endpoint recovery solution on more than 13,000 devices in more than 100 countries and plans to protect more than 26,000 endpoints when complete. The offering can be deployed on-premises or as a hybrid cloud or used by service providers. For backup and restore, all current releases of Windows, Mac and Linux OSs are supported. There is currently read capability for iOS, Android, and Research In Motion tablet and smartphone OSs for mobile access to protected data with the CommVault Access application. Global source- and target-side deduplication is included, and full-text search and reporting are available as options. The company is now in beta for its next generation of endpoint protection, targeted for release in 1Q13.

Return to Top

Copiun

Based in Marlborough, Massachusetts, Copiun is a venture-capital-funded company that designed from the ground up a laptop backup product called Copiun Data Manager and launched it in October

2010. The product targets midsize to large enterprises, with a rich set of capabilities, including efficient deduplication and backup completion during a few minutes of device idle time. Copiun Data Manager also stands out with its security features, such as a secure access gateway that allows VPN-less backup without opening a firewall port and native remote wipe features for tablets and smartphones, as well as its native e-discovery functions, such as full-text index and search and legal hold. Almost all its more than 200 customers use it for on-premises deployments, with the largest deployment being in the 30,000 range. Copiun has strategically decided to focus on on-premises deployments of larger enterprises and does not offer its own cloud. In September 2012, Good Technology acquired Copiun.

Return to Top

Datacastle

Datacastle is headquartered in Seattle. Datacastle Red (its endpoint backup offering) is sold primarily as a private label (EVault Endpoint Protection) through one partner, EVault, which in turn sells direct and through a broad range of service provider partners. Datacastle Red is offered as a service and is hosted on Microsoft Azure, so scale is being designed in but is yet to be proved as it is a relatively new offering. Most customers running Datacastle Red are implementing departmentally, with an average site deploying 150 users, but one customer acquisition of 6,700 seats is currently being deployed. Search is weak, with no full-text indexing, search of individual endpoints or federated search. Mobile devices are not supported. The Datacastle Red interface has been cited as easy to use and to administer. Client-side global deduplication is supported, as is autoresume of an interrupted backup. Two modes of remote wipe are supported: on-demand, where the administrator can initiate a remote wipe when the device is attached to the network; and automatic wipe of the system if it does not attach to the network within a certain time frame.

Return to Top

Druva

Druva is a startup located in Mountain View, California, that claims to have more than 1,300 customers with nearly 1 million endpoint devices protected. Backed by venture capitalists, the company launched its inSync endpoint protection product in October 2010. Gartner featured Druva in its Cool Vendors report for storage in 2012. In today's world, where endpoint protection has a lot of fragmented point solutions, such as separate products for mobile device management, backup and DLP, inSync stands out as a more unified solution that includes modules for backup, DLP (such as remote wipe and remote tracking of endpoint devices) and file sync/share. Its highly graphical user interface presents straightforward statistics and analytics for administrators and integrates all its modules. Druva can be deployed on-premises within an enterprise or as a cloud offering, which uses Amazon Simple Storage Service. It's also one of only two products among those profiled in this report that support iOS and Android backup.

Return to Top

EMC

EMC/Avamar

Avamar was acquired by EMC in 2006. Avamar is an enterprise server backup solution that also targets specific recovery use cases: VMware, network-attached storage, remote-office and branch-office, as well as endpoint backup. EMC claims to have more than 8,000 customers for all its Avamar configurations, and the offering can be deployed as on-premises or a hybrid cloud or by service providers to provide endpoint protection. Currently, EMC itself is the largest Avamar endpoint backup customer, with more than 38,000 users and growing. Avamar deduplicates backup data at the client (source) and globally across sites and servers and is one of the few implementations that utilizes variable block deduplication for greater data reduction. Windows, Mac and Linux laptops are supported today, with claims to support restore to iOS and Android in an upcoming release. Avamar can search on filenames, but it does not perform full-context indexing. More robust reporting may require the Data Protection Advisor add-on module. Avamar's Desktop/Laptop does not support integration with Data Domain or NetWorker, unlike all other Avamar products.

EMC/Mozy

Mozy was founded in 2005, is headquartered in Seattle, and was acquired by EMC in 2007. The company began as a consumer backup product, but with its acquisition by EMC, Mozy added a business/enterprise endpoint backup offering. Mozy claims to have a customer base of more than 80,000 business customers and more than 3 million total customers. The company offers backup service via a hosted model. Users can access their backups and synced files via iOS and Android devices. Full-text indexing and search of individual endpoints are supported, but not federated search or legal holds. Mozy supports single-instance store at the file level, but it does not provide block-level deduplication. Network throttling is supported, and CPU throttling is done by the user selecting impact on backup time and computer impact via a slider bar. Active Directory integration is in beta and is due to be delivered in the near future.

Return to Top

IBM

In 2005, an endpoint backup solution was delivered that integrates with TSM, which today is known as FastBack for Workstations and offers real-time, continuous data protection. FastBack for Workstations can be implemented stand-alone, as can the enterprise TSM Backup-Archive Client. However, IBM typically recommends that FastBack for Workstations and the TSM server be deployed together for endpoint backup to provide central administration of clients from the TSM administration center and integrated client-side TSM deduplication when data is sent back into TSM. Both on-premises and public cloud services available from IBM and its business partners are offered. Currently, one of the largest deployments has 7,500 endpoint devices actively in use as part of a 100,000-plus-device rollout that is in progress. When Fastback for Workstations is integrated with TSM, source data reduction includes compression and deduplication on client data, and data is further globally deduplicated on the target side on the TSM server. This configuration is limited to Windows support, with no current capabilities for Mac, Linux, iOS or Android devices, and full-text search is not offered. However, the TSM backup client by itself does support Mac and Linux in addition to Windows.

Return to Top