Cloud-based Backup and Recovery

By Earl Follis and Deni Connor

November 21, 2016

Sponsored by:

SSG-NOW TARGETED ANALYSIS

OUTLOOK REPORT

Contents

SSG-NOW TARGETED ANALYSIS

OUTLOOK REPORT

Cloud-based Backup and Recovery

Deni Connor, Founding Analyst
Earl Follis, Senior Analyst
November 21, 2016

Executive Summary

Cloud-based backup and recovery presents a significant opportunity for companies of all sizes to save money on their data protection capabilities or expand those capabilities at the same price. Given the cost savings of storing data in the cloud as compared to traditional on-premises data protection, some companies have even managed to save money while expanding their data protection capabilities.

Considering the compelling economic argument presented by cloud-based backup and recovery, every company should be weighing their options for a backup plan that assures timely protection of business-critical data. Many companies have struggled with the challenges required to formulate an effective backup and recovery strategy.

Among them are small businesses, which lack dedicated IT resources to implement, deploy and manage a comprehensive data protection platform. They also include enterprise-scale IT shops that have the expertise, but not necessarily the budget or bandwidth for implementing end-to-end data protection.

When considering backup strategies and vendors, we strongly recommend that cloud-based backup and recovery vendors be included in that evaluation. Many offer unlimited, continuous snapshots of virtual machines, applications and changed data. Others offer comprehensive recovery capabilities for specific business-critical applications, such as Microsoft Exchange. Cloud-based backup and recovery, whether a hybrid solution or a completely in-the-cloud solution, is a natural fit for most companies, if not as a complete backup strategy, at least for providing cost-effective backup coverage for many common environments and applications.

This report covers the history of cloud-based backup and recovery, common (and uncommon) features and capabilities of the capability, as well as best practices recommendations for companies looking to evaluate and implement a cloud-based data protection solution.

When Backup and Recovery isn't Disaster Recovery/Business Continuity

First off, let's define the terms we will be using and discussing in this report. Backup and recovery is typically defined as the ability to regularly and

automagically perform backups of business-critical and other data. As with traditional backup strategies and technologies, the ability to quickly and easily restore deleted, corrupt or misplaced files via a self-service process is of paramount importance in the cloud-based backup and recovery space as well. For the purposes of this report, we define backup and recovery as the process of storing and perhaps, archiving files on a regular basis, combined with the ability for self-service recovery and restoration of a file impacted by data loss of any kind.

Disaster recovery is one step beyond backup and recovery, offering the ability to not just restore lost data, but to also restore infrastructure component configurations, application data and database contents, such that you can restore applications, databases and other components back to a specific point in time or to a specific functionality. Usually this involves restoring your applications and components to just before the data loss event, whether those events are caused by natural disaster, software intrusions, hardware failure or human error.

Business continuity takes backup and recovery and disaster recovery one step further, restoring not just your computing resources to a specific point or place in time, but also restoring other aspects of business operations that can also be affected by a catastrophic data loss event. For instance, if a natural disaster, such as a flood or hurricane knocked out power to your data center and your company IT operations were plunged into darkness, you not only need a way to restore your IT infrastructure and applications to working order, but you also need to consider how your employees can continue to do their jobs if they can't physically make it to work or can't access critical IT resources due to a catastrophe. Business continuity includes considerations, such as work from home plans and capabilities for employees, failover to a backup telephone system so that you can still take calls from your customers and being able to process employee payroll following a catastrophic data loss event.

Driving Issues, Trends, History

Traditional disaster recovery is a very complicated, expensive proposition for most companies, a fact that put effective DR plans out of the reach of most small- and medium-sized businesses for several decades. As cloud computing has become more and more of a practical solution for myriad IT situations over the last five years, the advantages of cloud-based backup and recovery has become not just a possibility, but vendors in this market have introduced an amazing array of data protection features and capabilities while simultaneously dropping costs.

Now that your backup and recovery infrastructure can be hosted in a cloud (in addition to on-premises), companies that have traditionally spent heavily on data protection are now realizing substantial savings compared to traditional onsite backup strategies, such as big, expensive tape libraries or additional tiers of magnetic hard drive storage dedicated to backing up data centers and end-user computers.

Still today, most SMBs are either not backing up their business-critical data or else they were likely mismanaging their backups. Rotating tapes to offsite storage and managing those complex backup strategies were frequently a full-time job, and also a job that frequently no one really managed or thought about until a data loss event occurred.

Easy-to-use cloud-based backup and recovery has become a lifesaver for SMBs -- and even for some enterprises -- allowing more sophisticated backup and recovery processes at bargain basement prices. Companies that previously spent a fortune on backup and recovery have seen their backup capabilities increase while their costs went down. Other companies were able to keep their backup and recovery budgets static while greatly increasing the scope and depth of their data protection efforts. Enterprise IT shops have historically been better at protecting their server and application data from loss by spending lots of money and giving data protection a lot of attention. Enterprises recognize how devastating a data loss event can be to their business operations and because they can afford to develop a comprehensive data protection strategy, enterprises typically had better data protection in place than most SMBs. But many enterprise IT shops choose not to backup end-user data simply because of the enormous cost and complexity of managing those backup sets and frequent requests for restoration of lost end-user data. Cloud-based backup and recovery changes the question from 'How can we possibly afford to backup terabytes of end-user data?' to 'How can we possible afford to NOT protect end-user data now that it is economically feasible to do so?' Thus, even enterprises are taking advantage of economical cloud-based backup and recovery to protect data that heretofore has not been practical to protect.

Benefits of Cloud-based Backup and Recovery

Though we have already touched on some of the advantages to a cloud-based backup and recovery strategy for data protection, let's take a closer look at the various benefits your company can realize with a cloud-based solution.

Lowering data protection costs: By utilizing a cloud backup and restore infrastructure that is shared between thousands of customers, cloud-based backup and restore vendors can drastically drive down their costs and pass those savings on to their customers. Lowering data protection costs is the prime driver behind the proliferation of cloud-based offerings in the data protection space.

Offering backups where none existed before: Because of the lower costs of a cloud-based data protection strategy, companies that previously found on-premises data protection to be a cost-prohibitive proposition can now leverage cloud-based alternatives to streamline their backup and restore operations. This allows companies to protect end-user data, non-production server data and other data repositories that were previously unprotected or only backed-up on best-effort basis.

Relieving backup admins of backup/restore workload: Thanks to the ease-of-use among most cloud-based backup and restore offerings, self-service data protection is now a viable option for companies of all sizes. This puts end-users in the driver's seat for their own data protection, allowing users to customize the scope of their backups--within certain company guidelines--and perform their own restores on demand. Ask any help desk

agent or backup admin what their biggest time sink is and they'll usually identify performing end-user restores as a tremendously time-consuming affair. Cloud-based data protection offers a better solution.

Reliability of the backup process: In general, once your cloud-based backups are properly configured, that process will continue on the appointed schedule for as long as the backup source exists. This takes away the worry that backups are being run on-time and successfully each and every day. Backup admins and other operations personnel can now change their focus to higher-value activities now that the day-to-day process of backup and restore has been automated. There will still likely be occasions when end-users require an admin to intervene in the process but for most backup sources, the cloud-based backup and restore process empowers end-users to manage their own data protection.

Auto-scaling of backup storage resources: One of the biggest problems with on-premises storage of any kind of data is the ever-expanding amount of data that is being amassed by companies of all sizes. By leveraging a cloud-based backup and restore strategy, your backup vendor will handle scaling, availability and redundancy of cloud resources to ensure that sufficient storage is always available to the installed user base. Another related benefit to cloud-based backups and restore is that some vendors price their products based on the amount of data stored in the cloud. Only paying for what you use can save companies significant costs over provisioning their own on-premises storage array to handle backups. Such arrays are usually underutilized right up until the moment when they start to become oversubscribed, when more storage resources must be ordered and implemented, an expensive and complex process.

Automatic offsite storage of backups: Those of us who can remember putting our local backup tapes in a briefcase to take home or handing them to an offsite data archiving company will appreciate the fact that cloud-based data protection offers offsite data storage as part of the architecture. If your chosen cloud-based backup and restore vendor replicates your data to multiple geographically-disparate clouds, you are not just getting offsite storage, you're getting offsite storage and replication, an additional layer of data protection for your business-critical data.

Lower TCO: Not only is cloud-based data protection cheaper than traditional backup and restore options, but looking at the bigger picture of total costs related to backup and restore activities, cloud-based data protection has the potential to greatly reduce the TCO on your backup infrastructure. Yes, licensing will be cheaper with cloud-based data protection but also consider that the amount of time spent administering the backup environment will likely be lower. Self-service backups and restores will also lessen the load on your help desk staff. Knowing that your cloud-based data protection vendor is responsible for scaling

your cloud storage, you will undoubtedly save money over deploying more expensive storage arrays with greater and greater capacity in your data center.

No need to rip and replace: Cloud-based data protection can almost always be implemented in a phased fashion, such that you don't require a single switchover from the previous backup and restore strategy to the cloud-based strategy. As agents and appliances are installed, you have complete control over which computers are transitioned to the new platform and most importantly, when that transition occurs. This flexibility makes implementations much easier and less stressful compared to a hard cutover from an old to new infrastructure.

Compatibility: Another key advantage to cloud-based data protection is compatibility with your existing backup hardware and storage gear. You don't have to upgrade your storage to utilize it with a hybrid approach, nor do you have to decommission existing tape drives and other backup components in order to implement cloud-based data protection. This compatibility allows IT shops to make independent decisions about when backup equipment is decommissioned or phased out if the new cloud-based architecture is compatible with your existing infrastructure.

Elements of Cloud-based Backup and Recovery

The elements of a successful cloud-based backup and recovery strategy may include components such as a software agent installed on the computers being protected, a physical or virtual backup appliance that serves as a gateway to the cloud, and in a hybrid scenario, some amount of local storage that caches data bound for the cloud or serves as on on-premises repository for data backups. In many cases, that local backup appliance can include capabilities, such as generating bare metal restore disks, encryption of data and management of the backup and restore processes both locally and in the cloud.

Agents are small pieces of code running on target computers that facilitate communication and management tasks between the computer being protected and the nearest backup appliance. Agents give your backup appliance and/or management software access to the local resources of a protected computer. Be sure to evaluate agent technology for any cloud-based backup vendors you are considering implementing to ensure that they provide all of the necessary capabilities without burdening your protected computers with a CPU- or memory-intensive piece of software that can affect performance of the protected computers.

Local backup appliances can serve as a caching mechanism for data destined for the cloud, a point of presence on the local network to facilitate management of your backups and restores and other capabilities such as generating bare metal restore disks. Depending on your backup vendor and the capabilities of their appliance, you may also be able to configure your appliance to attach to multiple

clouds, to attach to other appliances in other locations or to attach to local storage in hybrid cloud architectures.

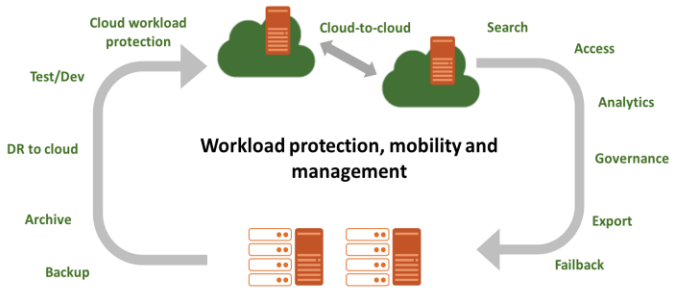
For vendors who support the creation of a baseline backup that can be burned to disk then mailed in to the vendor to seed their initial backups more quickly, the local appliance typically provides that initial backup process and creation of the backup set that can be burned and mailed in.

Bare metal restores are a process that generates a bootable disk that includes the base operating system along with some or all of the protected data on a computer. Your cloud-based backup vendor may generate bare metal restore disks upon request following a data loss event, in this case, typically a server hardware or disk failure that requires a new server to be built from scratch. The bare metal restore disk shortens the amount of time it takes to deploy and configure a brand new or un-provisioned replacement server to take over for a server sidelined by hardware failure(s). In many cases, your cloud-based backup vendor may leverage the local appliance to burn bare metal restore disks on the appliance itself. Otherwise, your backup vendor may overnight that bare metal restore disk to you upon notification that you've suffered a data loss event and need to re-provision a replacement server from scratch.

Use Cases

With virtues such as low cost and ease of use, cloud-based backup and recovery is a natural fit for many data protection scenarios.

Follow us through several use case scenarios that exemplify where, when and how you can leverage cloud-based backup and recovery options to improve your data security and provide an easy, seamless method for restoring files that are lost, infected or corrupted for any reason.



Server data protection

SMBs - Server data protection is a prime application for cloud-based backup and recovery, as SMBs have traditionally struggled with server data protection, due to both complexity and cost. Installing an agent on a server is a relatively easy and painless process and once that agent is installed, you can configure it for the frequency of backups and where that data may be stored. In smaller server environments, there may not be a need for a backup appliance; the server agents can backup and restore directly to a cloud. The self-service nature of cloud-based backups is a natural fit for SMBs, where having IT staff dedicated to performing server backups is likely cost-prohibitive.

Enterprises - Considering that most enterprise-sized companies already have sophisticated backup and recovery procedures in place for their production servers, the casual observer might assume that cloud-based backup and recovery has no place in the enterprise IT space. But you'd be wrong if you make that assumption. Many enterprise companies do not put a priority on regularly backing-up non-production servers, such as development and test servers. Here is where the low-cost of cloud-based

backup and recovery shines, even in enterprise IT shops. Low-cost cloud backups can save hours or even days of reconfiguring a non-production server after a data loss event. The self-service aspect of cloud-based backups also appeals to developers and operations personnel who manage those non-production servers. Cloud-based backup and recovery offers a compelling value for non-production servers, even in the enterprise data center.

Self-service end-user backups and restores

Another compelling use case for cloud-based backup and recovery is to allow and support self-service backups of end-user data.

SMBs - For SMBs, self-service backup and restore fits well in environments where there is no staff available or dedicated to managing end-user backups. In these cases, self-service use of cloud-based backup and recovery is almost an operational requirement to ensure ongoing business operations can continue in a timely fashion after a data loss event.

Enterprises - For enterprises that don't currently backup end-user data at all, the justification for that gap in data protection is simply because backing-up end-user data is considered too costly and complex to protect on a company-wide basis. Of the burdens for enterprise backup admins, the most pronounced is the time-consuming task of helping end-users restore data after a data loss event. Easy-to-use self-service backups and restores solves that problem. Cloud-based backup and recovery is a natural fit for these situations where low-cost, easy-to-use, self-service data protection allows enterprises to protect data they can't or won't protect at a global level. The combination of low cost and ease-of-use combine to make self-service end-user data protection a natural fit for SMBs and enterprise-size businesses alike.

Archive in the Cloud

Cloud advantages are near-infinite scalability and end-user management choices from hands-on to set-and-forget. This makes the cloud a good choice for infrequently accessed cold or archive storage; not so good when the user needs frequent recovery or has a project requiring large data access, such as an eDiscovery collections phase. End-users should do due diligence on entry and projected costs and data access times on cloud-based archive storage.

Amazon Glacier and Google Nearline are popular public cloud offerings for cold storage. Be aware that with Amazon Glacier, users are looking at a retrieval times in hours. For some, restores like eDiscovery search results, this timeframe is acceptable; for other situations, like delivering digital assets to a waiting creative team, it is not. Google's Cloud Storage Nearline stores data at the same low price that Amazon does and restores data within minutes. Like Amazon there are additional retrieval costs. Many MSPs also offer archive storage-as-a-service in their own clouds or in hosted environments on Amazon, Glacier, Azure, Rackspace and other providers.

Archive Storage as a Service

Data backup and archiving is a popular MSP service offering, but the truth is that profit margins can be very thin. Archive Storage as a Service can be a profitable offering to customers who need inexpensive cloud-based cold storage with retrieval times under a day. By adopting low-cost object-based storage with a multi-

tenant infrastructure, the MSP can offer cold storage services at a reasonable profit.

Remote Office/Branch Office

Remote office and branch office (ROBO) use cases are a perfect fit for cloud-based backup and recovery. Assuming that you deploy a ROBO backup and recovery solution featuring an easy-to-use user interface and either a virtual or a physical backup/restore appliance onsite at the ROBO, IT can configure backups and restore files without requiring intervention from onsite personnel. Comprehensive remote management features of the appliance is also a must-have for ROBO operations, so that all management tasks can be completed over the network, rather than requiring someone to manage the device onsite. Having a cloud-based backup and recovery appliance onsite improves running times for backups and speeds the restoration of files from either local or cloud backup sets using deduplication and compression of data flowing to and from the cloud.

Disaster Recovery

Disaster recovery (DR) also presents a strong use case example for cloud-based backup and recovery. With many such solutions, the backed up image can be booted directly in the cloud, as part of a DR strategy so that operations can continue until the crash or disaster is addressed. Rather than struggling to repair or replace misbehaving hardware or software in order to recover from a catastrophic server crash, you can leverage your backup and recovery appliance to very quickly boot-up virtual servers to replace servers, either physical or virtual, that have been affected by an issue of outage. Note that not all backup and recovery solutions support these types of DR features. If this is an important consideration for your company, be sure to evaluate potential solutions with those capabilities in mind.

Workload Mobility

Similar to using cloud-based backup and recovery for DR purposes, these solutions can also offer workload mobility. This gives organizations the flexibility to quickly replicate as needed and spin up instances in the cloud for test and dev purposes. Or, to move workloads to different cloud regions to optimize accessibility, continuity or data residency needs. With this ease of use, businesses no longer have to tie their data to hardware and can easily replicate and migrate as needed.

Governance

Governance and corporate compliance has become a business-critical area of concern for most companies over the last 10 years. Now that senior company executives must certify that all applicable governance requirements are met on an on-going basis, being able to satisfy data retention requirements via a backup and restore solution allows IT admins and business management to solve two or more problems with one system. The IRS typically requires entities to retain financial data for at least seven years and other governance regulations, such as FINRA or Sarbanes-Oxley, may have even longer retention horizons. Government regulations such as HIPPA have very stringent requirements for the security of personally identifiable information (PII), so ensure that your backup and recovery solution supports strong encryption and data security technology.

Considering the high stakes in corporate compliance and governance regulations, the cost of a backup and restore solution that helps a company meet or exceed its regulatory requirements can be a very small price to pay.

Best Practices for the Implementation of Cloud-based Backup and Recovery

Some of the best practices involved in evaluating and implementing a cloud-based backup and restore strategy are common to almost any type of IT project. But the specifics of cloud-based data protection include some unique situations and techniques that you will only have to consider with a project of this type. Here are our recommendations for the most important things you can't forget to remember when implementing cloud-based data protection software and hardware.

Planning: If you fail to plan, you plan to fail. Always have a project plan, even if it is an informal document or written on the back of a napkin, to guide your evaluation, procurement, implementation and support of your cloud-based backup and restore strategy. As part of your plan, outline who is responsible for the various aspect of a successful implementation, what happens when something goes wrong, plus how and where users can get support for their backup and restore issues.

Architecture: Cloud-based data protection can run on a variety of architectures, including direct-to-cloud, hybrid with caching, hybrid with storage and a local appliance to cloud. Here is a closer look at each option:

Direct-to-cloud - In simple or smaller environments, you can deploy data protection agents that communicate directly with cloud resources provided by your backup and restore vendor. Those agents access cloud resources without the need for a local appliance coordinating backup and restore operations. Advantages include lower cost of ownership due to no local appliance required and a very simple architecture. Disadvantages may include lack of effective management and monitoring capability among these standalone agents and the possibility of redundant connections to the internet to ensure that data is always flowing to and from the cloud as expected.

Hybrid with local caching - Hybrid architectures with local caching require a local appliance with sufficient memory and disk resource to serve as a cache for data destined for the cloud. If network bandwidth between the appliance and the cloud is restricted or overloaded, the appliance will cache that data locally and upload it to the cloud as capacity allows. Cached data is usually deleted from the local appliance as soon as it has been successfully uploaded into the cloud.

Hybrid with local storage and cloud archiving - Similar yet different from the previous example, another hybrid scenario features a local appliance with local storage serving as a gateway that supports cloud archiving. This architecture allows for tiering of data based on criteria that you can configure, e.g., age of file, last access date, frequency of access and business-critical or performance-related characteristics. Not all vendors support this type of scenario and those that do offer a variety of configurations and options for tiering your data exactly as required.

Testing: Thoroughly testing all candidate products for your cloud-based data protection solution will ensure that there are no surprises during implementation or operational phases of the project. Have real end-users test the backup and restore process for each of your candidate products. If you are implementing backup and restore capabilities for servers, be sure to include server and backup admins in your evaluation and testing phases. For whatever data protection problem you are trying to solve, allowing your backup and restore 'customers' to test all options and participate in the selection process is highly advisable, when possible.

Encryption: Data security is just as important to your company's success as data protection. With that fact in mind, be sure that any cloud-based data protection products you evaluate include appropriate encryption capabilities for your company's requirements. Many companies are subject to governmental regulations on data security and privacy, such as HIPAA, FINRA and Sarbanes-Oxley. Be sure that any cloud-based solutions you evaluate include the appropriate level of encryption (both in-transit and at-rest) and sufficient data security features to ensure compliance with all applicable rules, regulations and company guidelines.

Seeding of backups: Most cloud-based backup and restore vendors have the ability to make an initial full backup of server data that would take too long to upload to the cloud via the local appliance with a WAN connection to the internet. That initial full backup might be captured and burned to disk by a separate utility or that capability might be part of the appliance feature set. Once you have backup disks burned and sent to your vendor, they will load those backup sets into their cloud and all backups going forward will be incremental backups. This saves days or maybe weeks of uploading to get that initial backup. Seeded backups for end-user computers are usually not as critical, simply because the amount of data to be protected is likely considerably less than that found on a server. Note that if you do have end-users with a large amount of business-critical data stored locally, you can opt to seed their initial backup set via a disk backup just as you would a server.

Bare metal restores: Bare metal restores are bootable disks with a recent copy of both the underlying operating system (OS) and all configuration data for a specific server. Bare metal restore disks might be created by the vendor at a central facility and overnighted to the customer after a data loss due to hardware failure or hacking. Or, their local appliance may be able to burn the bare metal restore disk on an on-demand basis. Obviously, this capability might save you hours or even a day or two in recovering from a server crash or other catastrophic server mishap. Look for a vendor with a continuous and automatic updating of bare metal restore disk data from all protected servers. That will save you from having to locate all of the OS disks that came with the server (if you even received OS disks), install the OS from scratch then apply all required patches, properly configure the server then reinstall all applications and supporting software. This can be a very time-consuming process and the last thing you want to attempt when you have a critical server that is sitting in the dark in your data center. Bare metal restores are your key to a timely restoration of servers after a hard crash.

Cloud backup redundancy: In addition to the ability to tier data between local storage and cloud

storage, some cloud-based data protection vendors also offer the ability to replicate backup data between other data centers and also between multiple clouds. Some local appliances installed in company-owned data centers can replicate data between multiple data centers--with a similar appliance in each--to give you geographic redundancy of backup data. Some vendors also offer the ability to connect one appliance to multiple cloud instances, to distribute or replicate business-critical data between disparate clouds or disparate locations.

Support: All of the bells, whistles and capabilities of cloud-based data protection are worthless if you as the project manager or operational IT manager cannot get help from the vendor, when needed. We always recommend that you include a full test of each vendor's support processes and expertise as part of any product evaluation. Online knowledge-bases and a fancy support portals are great and can be both a learning experience as well as a lifesaver, but you also need to be able to reach a real person in a timely manner, and that support agent must have the expertise to fix your problem or find someone who can. When testing and evaluating your options, be sure to test the vendor's actual customer support mechanism, not just the typical handholding of a pre-sales engineer. Once you buy a solution, you need to know that the company will continue to stand behind their product and fix things when they go awry.

Why Should You Care

Cloud-based backup and restore is now revolutionizing the data protection space and becoming a compelling value proposition for SMBs and enterprise IT shops looking to prevent data loss via the insurance offered by cloud-based backup and recovery. From small mom and pop shops, whose businesses would be decimated by a significant data loss event, all the way up to multi-national conglomerates who have been forced by budget to restrict the amount of data they protect, cloud-based backup and recovery is the no-brainer solution to expensive traditional data protection schemes or the more common total lack of data protection for smaller concerns operating on a limited budget. Considering that industry experts estimate that more than 70% of businesses hit by a significant data loss event go out of business within 18 months--and we saw just such devastating impacts to local businesses after the 9/11 attack in New York City--data protection has gone from an expensive nice-to-have to a budget-friendly, business-critical process that is just as important as the underlying data is to continuing company operations.

In short, if your company is not currently taking advantage of cloud-based backup and recovery offerings, you should locate and implement a suitable data protection solution as soon as possible. Literally, the survival of your company could be at stake. If you work in a company that has a data protection strategy in place, you owe it to your staff and your budget to explore the possibility that cloud-based backup and recovery can save you significant money or allow you to increase your data protection umbrella without increasing your costs. In some cases, you'll be able to do both. We highly recommend that you explore what all of the fuss is about in cloud-based data protection and leverage these incredible capabilities to better protect your business-critical data. It's no longer a question of can you afford it; it's now a question of can you really afford not to?

SSG-NOW TARGETED ANALYSIS

OUTLOOK REPORT

druva

Vendor Name: Druva

Product Name: Phoenix, inSync

Link to website: www.druva.com

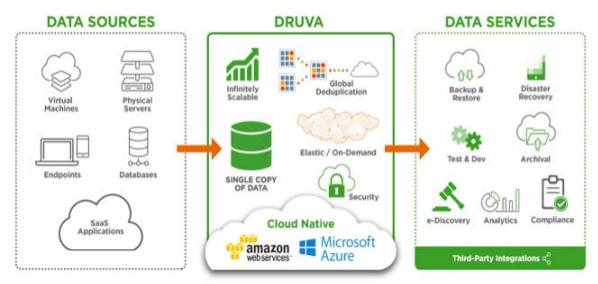
Links to datasheets:

inSync:
http://pages2.druva.com/rs/druva1/images/Druva-inSync-Enterprise-Endpoint-Data-Protection-Governance.pdf
http://www.druva.com/documents/Druva-inSync-Microsoft-Office-365-Datasheet.pdf

Druva CloudCache:
http://www.druva.com/documents/Druva-CloudCache-Datasheet.pdf

Druva Phoenix:
http://www.druva.com/documents/Phoenix-DRaaS-Disaster-Recovery-in-the-Cloud-datasheet.pdf
http://pages2.druva.com/rs/druva1/images/Druva-Phoenix-Simple-Server-Backup.pdf

Product and Technology: Druva offers two SaaS-based services technologies and one on-premises software-based cloud caching appliance: Druva inSync, Druva Phoenix and Druva CloudCache.



Druva inSync

Druva inSync is a unified data protection solution for Windows, iOS, OSX, Android and Linux endpoint devices and cloud-based

applications, such as Office 365, Exchange Online, Box and Google, that is delivered through a Software-as-a-Service (SaaS) model.

The SaaS model allows for centralized policy management and device controls and is configurable for regional and international privacy and storage requirements. Among the policy management capabilities is the ability to migrate data and perform self-service data refreshes. In addition, inSync provides data loss prevention (DLP) features like remote wipe, geo-location and encryption of laptops and smart devices. It also, unlike its competitors, provides integrated file sharing and collaboration of documents.

Data governance capabilities are also included within inSync and help organizations deal with challenges such as exiting employee risks, data spoliation, and the mass export of forensic data. IT can perform federated searches across all end user data, collect data and store it for legal and compliance purposes, and identify and remediate violations involving at-rest sensitive data, such as PHI, PII or PCI. Data on legal hold is stored in-place, avoiding the risk of data spoliation and the additional costs of forensic data storage. Immutable audit trails ensure that all data activities are logged.

inSync uses patented, source-side global data deduplication to provide efficient storage and bandwidth reduction; security in the form of data scrambling and encryption; and support for Amazon Web Services and Microsoft Azure.

The scale-out inSync architecture isolates metadata from the data blocks themselves, ensuring the use of multiple workflows from the same dataset. This facilitates IT managing all the organization's end user backup and restores, governance needs, and file sync and share capabilities from a single dashboard.

inSync provides file-level recovery, which is critical for organizations using backup to recover from a ransomware attack.

Further, optional on-premises caching capability – called Druva CloudCache -- allows high-performance data handling and scheduled cloud synchronization, combining LAN performance with WAN bandwidth maximization for ultimate flexibility.

Several different models of Druva inSync are available, including Business, Enterprise, Elite and Elite Plus, each available at different price points and capabilities. CloudCache is included in the Elite and Elite Plus versions of Druva inSync.

In addition, Druva provides a private cloud version of inSync that operates on-premises and includes backup and recovery of desktops, laptops and mobile devices, data loss prevention, file sync and share, and eDiscovery enablement.

Druva inSync is licensed on a per-user basis.

Druva Phoenix

Druva Phoenix focuses on the server-side of the data protection equation, in particular on remote and branch office servers, which run as physical or virtual servers. Like Druva inSync, Phoenix is an architecturally similar SaaS-based software that leverages Amazon Web Services as if it was

a native operating system. While Phoenix is not as full-featured in the data governance space as Druva inSync, the platform is moving in that direction.

Druva Phoenix supports Linux and Windows file servers, SQL Server, and virtual environments. It includes global server-based deduplication for data reduction and efficient, auto-archiving of data and VMware file-level recovery.

Designed for cloud backup, archiving and long-term retention, disaster and ransomware recovery and test/dev instances. Druva Phoenix can failover to the cloud or to the CloudCache appliance, as well as replicate and rollback to previous versions as needed.

Druva Phoenix is available in three models – Business, Enterprise and Elite. Phoenix is based on a consumption model that is measured in TB consumed. Licensing allows for flexible pricing in which under-run credits are rolled over and applied for capacity management increases. CloudCache is included in the Enterprise and Elite versions of Druva Phoenix.

Druva Phoenix uses a consumption-based pricing model.

Druva CloudCache

CloudCache is a software-based appliance that is installed on-premises between the network and the corporate firewall and the Druva cloud. It enables IT teams to avoid using precious bandwidth during peak usage times and offset the migration of data to the cloud to a time that best suites the specific needs of their network. The CloudCache appliance also assists with unpredictable and low bandwidth in the initial seeding of the cloud with backup data and in the mass restores of data during device refreshes.

CloudCache can also be used for block transfers between the server and the cloud, for local restores of data cached on the appliance and for quick access to legal hold information.

Company Philosophy: Druva is an early innovator in endpoint backup and data governance and a leader in remote office server data protection and information management. The company leverages the public cloud to offer a single pane of glass to protect, preserve and discover information. Druva's software intelligently collects data from wherever it resides – endpoint devices, in-the-cloud applications or remote/branch office servers -- and unifies backup, disaster recovery, archive and governance capabilities into a single dataset.

Corporate: Druva was founded in 2008 by CEO Jaspreet Singh, CTO Milind Borate and Ramani Kothandaraman, all formerly of Veritas, as a time-indexed file system solution for endpoints, on-premises datacenter-focused data protection. Subsequent to its founding, the company in 2012 introduced a cloud-based data protection architecture called inSync that protects, preserves and allows discovery and compliance of endpoint devices and cloud applications, such as Office 365, Exchange Online, Google and Box, for corporate governance purposes.

In 2014, Druva extended its portfolio of data protection and governance solutions with the

introduction of Phoenix, a SaaS application that provides physical and virtual server deduplication, backup and recovery, disaster recovery, data governance and archive capabilities.

The company is funded for $118 million by Sequoia Capital, Nexus Venture Partners, Blue Cloud Ventures, Tenaya Capital, NTT Finance, Hercules Capital, EDB Investments, EMC Ventures and Indian Angel Network.

Among Druva's 4,000 customers are 7Eleven, Clorox, Continental, Deloitte, DHL, IKEA, ING, Marriott, NASA, NBC Universal, Pfizer, PricewaterhouseCoopers, ServiceNow, Schlumberger and Stanford University. The company's technology manages and protects over 25PB of source data.

The company counts among its partners Amazon Web Services, Microsoft, OpenText, AccessData, DISCO, MobileIron, MaaS360 and VMware Airwatch.

Druva has 410 employees and offices in seven United States and international locations. The company is headquartered in Sunnyvale, Calif.

SSG-NOW Take: Druva is differentiated by its cloud-native architecture, which uses patented deduplication technology to reduce the data sent across the network to the cloud, saving on storage and bandwidth costs. The Druva platform brings together multiple, global workloads into a single console, streamlining data protection and management for IT.

On the end user side, Druva is differentiated from its endpoint data protection competitors by the inclusion of data governance in its SaaS-based data protection software, and by its support for enterprise sync and share capabilities.

Druva inSync is a proven SaaS offering that reduces the cost of eDiscovery and data collection, reduces IT support costs and increases IT productivity and eliminates infrastructure investments for not only data protection, but archiving and data governance purposes.

Druva Phoenix extends the Druva platform to data on physical and virtual servers. IT can manage data across any number of remote office locations via a single dashboard, and restore data without requiring any on-site resources. Often complicated actions, such as spinning up instances for DR or test/dev needs can be done near-instantaneously.

Druva Phoenix's consumption-based pricing structure saves organizations from having to make initial costly investments and easily scale their storage as needs change. Organizations report saving as much as 80% on their storage and bandwidth costs.

As more and more companies move to the cloud, deployment of both Druva inSync and Phoenix will both complete and complement their data protection, archiving and data governance strategies. ●

SSG-NOW TARGETED ANALYSIS

OUTLOOK REPORT

Druva Phoenix and inSync – Features and Capabilities

	Product Name	Consumption Type (Disk, Tape, Cloud, Hybrid w/ on-premises appliance)	Data Centers Supported	Backup Type (Full, Incremental, Synthetic, Other)	Cloud Gateway Included	Agent Required	Included/Optional	Agent Type/ Support for
Druva	Phoenix	C, H	AWS S3, Glacier	F, ever-incremental	N	Y	I	Windows, Linux, VMware (By proxy) MSQL
Druva	inSync	D, C, H	AWS S3, Microsoft Azure	F, ever-incremental	N	Y	O	Windows, OSX, Linux, iOS, Android

	Product Name	Type of Offering	Details
Druva	Phoenix	BaaS, DRaaS, STaaS, SaaS, Iaas	BaaS: Price based on storage consumed. Optional CloudCache software appliance available. Stores all data at an internet facility, Jobs scheduled, Changes to files don't trigger backup. DRaaS: Converts VM images to AMIs and facilitates spin-up within customer AWS instance. STaaS: Can be used for long-term data retention and offsite data protection.
Druva	inSync	BaaS, STaaS, SaaS	BaaS: Licensed per user/per month. Stores all data at an Internet facility. Optional CloudCache software appliance available. Scheduled jobs. Backups not triggered by changes to files. Provides HA through data center replication provided by AWS and Azure. STaaS: Can be used for long-term data retention and offsite data protection. SaaS application support: Office 365, Salesforce, Box, Google and Exchange Online

		Encryption	User-owned keys	Physical server backup	Microsoft Exchange	SQL Server	SharePoint	Network Attached Storage	VMware virtual machines	Hyper-V	VStorage API support	Image-level backup	File-level recovery	Block-level Backups	Changed block tracking	File-by-file restore	User self-service	Data compression	Differential data compression	Bandwidth throttling
Druva	Phoenix	Y	Y	Y	N	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Druva	inSync	Y	Y	N	Y	N	N	Y	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y

		Offline backup	Jobs scheduled	Backup triggered by changes to files	File synchronization	Dataset Seeding	Cost	Bulk restore	Centralized mgmt console	File retention policies	Proactive monitoring	High availability	High availability method	Cost	# of availability zones	Versioning
Druva	Phoenix	Y	Y	N	N	Y	N/A	Y	Y	Y	N	Y	Via AWS	I	3 per storage region	Y
Druva	inSync	Y	Y	N	Y	N	N/A	Y	Y	Y	Y	Y	Via AWS and Azure	I	3 per storage region	Y

		Open files	# of backup sets	Support for Veritas OST	Snapshots	Price	Any point in time	Hardware agnostic	Bare Metal Recovery Included/Optional	Price	Bootable CD	Recover to similar hardware	Recover to identical hardware	Recover to Virtual environments	File and folder recovery
Druva	Phoenix	Y	Unl.	N	I	As low at $6/user/ month	Y	Y	N	N/A	N/A	N/A	N/A	N/A	N/A
Druva	inSync	Y	1	N	I	As low as $0.003/GB/ month	Y	Y	N	N/A	N/A	N/A	N/A	N/A	N/A

		Deduplication Included/Optional	Price	Type (Source, Inline, Target, Post-processing)	Appliance	VTL support	NAS Support	Symantec OST	Fibre Channel
Druva	Phoenix	I	N/A	S	N	N	N	N	N
Druva	inSync	I	N/A	S	N	N	N	N	N

		Continuous Data Protection (Included/Optional)	Price	Any-point in Time	# Snapshots supported	Microsoft Exchange	SQL Server	SharePoint	Virtualization	# Servers supported	# of Desktops Supported
Druva	Phoenix	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Druva	inSync	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

		Channel (Direct, MSP, Hosted service Provider, Online/cloud, VAR, Corporate/Govt Disty)	Pricing	Notes
Druva	Phoenix	D, MSP, O, VAR, Corp	Price on capacity and licensed as a subscription; Priced on 1 hour RPO and RTO in minutes	Pay-as-you-go. Also supports AWS GovCloud. Uses auto-tiering and leverages Amazon Glacier. Optional CloudCache for storing data locally for later migration to Amazon S3.
Druva	inSync	D, MSP, O, VAR, Corp	Amount of data being backed up, Number of users, per user subscription model	Supports AWS GovCloud. Optional CloudCache for storing data locally for later migration to cloud. Also includes remote file access, governance and compliance management.

About SSG-NOW™

SSG-NOW is an industry analyst firm focused on storage, server, cloud and virtualization technologies. Our goal is to convey the business value of adopting these technologies to corporate stakeholders in a concise and easy-to-understand manner.