

OUTLOOK REPORT



Cloud-based Backup and Recovery

By Earl Follis and Deni Connor

November 21, 2016

Sponsored by:  **DataVault**

This report is presented by USDV, who understands and agrees that the report is furnished solely for its distribution to customers and sales team, without the prior written consent of Storage Strategies NOW.

SSG-NOW | 8815 Mountain Path Circle | Austin, Texas 78759 | 512.345.3850 | SSG-NOW.COM

Note: The information and recommendations made by SSG-NOW, Inc. are based upon public information and sources and may also include personal opinions both of SSG-NOW and others, all of which we believe are accurate and reliable. As market conditions change however and not within our control, the information and recommendations are made without warranty of any kind. All product names used and mentioned herein are the trademarks of their respective owners. Storage Strategies NOW, Inc. assumes no responsibility or liability for any damages whatsoever (including incidental, consequential or otherwise), caused by your use of, or reliance upon, the information and recommendations presented herein, nor for any inadvertent errors which may appear in this document. Copyright 2016 All rights reserved. SSG-NOW, Inc.

Contents

Executive Summary	2
When Backup and Recovery isn't Disaster Recovery/Business Continuity	2
Driving Issues, Trends, History	3
Benefits of Cloud-based Backup and Recovery	4
Elements of Cloud-based Backup and Recovery	6
Use Cases	7
Server data protection	7
Self-service end-user backups and restores.....	8
Archive in the Cloud.....	8
Disaster Recovery	9
Best Practices for the Implementation of Cloud-based Backup and Recovery	10
Why Should You Care	12
USDV Cloud Continuity Program	13-42
USDV System 2 MAX Specs	43-50
Why USDV.....	51

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 possibly 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 an 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.

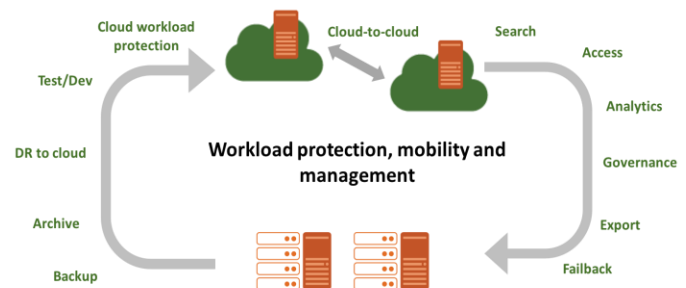
Bare metal restores are a process that generates a bootable disk that includes the base operating system along with some or all of the protected data on a computer. Your cloud-based backup vendor may generate bare metal restore disks upon request following a data loss event, in this case, typically a 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 like USDV 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 HIPAA 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 fail within 18 months**. And we recently 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 idea 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?

Call USDV today for help in getting started!



Marc Shaffer June 6, 2016

US DataVault Cloud Backup and Disaster Recovery

Direction



US DataVault Customer Commitment



US DataVault Customer Commitment

- Always free trial*
- Always free training*
- Always free Certification*
- Always free startup*
- Always free Server software (unlimited)*
- Always free Workstation software (unlimited)*
- Always free Application Software (unlimited)*

- No minimum amounts*
- Never any startup costs*
- The very best Support in the Industry!*
- VERY Feature rich!*

Our Business is Keeping YOU in Business!



US DataVault Customer Commitment

– *SPLA pricing*

– *The Storage Based Licensing works according to an SPLA model, based on the actual used gigabytes posted from the storage server at the end of every month. The actual storage usage is calculated:*

- *After compression at the client side*
- *After de duplication at the client side*
- *Including retention*



US DataVault Cloud Backup and Disaster Recovery



US DataVault

Fast, Easy, Secure, Reliable, Complete & Affordable!

- *Microsoft, Apple, Linux*
- *32 and 64 bit*
- *File, Folder, Volume, System*
- *Open file support*
- *System State*
- *Exchange 2003 2007 2010 2013*
- *MS SQL 2005, 2008, 2012*
- *SharePoint 2010 and 2013*
- *Oracle 11g*
- *MySQL Microsoft, Apple, Linux 5.0, 5.1, 5.5, 5.6*
- *VMware including CBT and De Dupe 4.1, 5.0, 5.1, 5.5*
- *VMware per file restore*
- *Hyper-V 2 & 3*
- *Hyper-V Cluster Shared Volumes (CSV) support*



US DataVault

Fast, Easy, Secure, Reliable, Complete & Affordable!

- *Local backup (USB or NAS) and Cloud*
- *Multi thread support*
- *Network shares*
- *Client side de duplication*
- *Pre processing of data 8 mb blocks*
- *Dual bandwidth throttling*
- *Auto update of clients*
- *Detailed reporting*
- *Audit trails*
- *Encryption 128, 256 and 448 blowfish*
- *In flight and at rest*
- *Autotask*
- *ConnectWise*
- *Supported Languages, English, Dutch, Russian, German. Spanish, French, Italian, Japanese and Swedish*



US DataVault

Fast, Easy, Secure, Reliable, Complete & Affordable!

- *Virtual Disaster Recovery VDR*
 - *VDR Restore Physical to Virtual VMware or Hyper-V*
 - *Local or Remote Hot VMware 4.1,4.5,5.5 Hyper-V*
 - *Customer Site, Your Site or Continuity Cloud (SLC)*
- *Bare Metal (similar) for now*
- *Branding/Skinning*
- *Deep Branding*
- *Client self healing,*
 - *local database w auto backup*
 - *Cleaning*
 - *Branding*
- *Runs as a Service*
- *Full API*
- *Virtual Drive*
- *WebDAV*



Protect

- EFI BIOS / GPT Partition Support (for BMR and VDR)
- Alternate Backup Credentials

Recover

- LocalSpeedVault configurable for VDR
- Easy VMware Restore

Performance &
Scale

- Multi-threaded Restores
- Skip File if Exist during restore (FS, Share, SQL, SharePoint, Hyper-V)

Usability &
Manageability

- Redesigned HTML Backup Manager
- Remote Client Discovery and Deployment (Windows)
- Backup Coach



Protect your users and your Business



Alternate Backup Credentials

Allows the use of alternate credentials if the default account has insufficient rights to protect a resource.

Benefit: Improved resiliency and a higher percentage of successful backups

Virtual Disaster Recovery Enhancements

Access to configure LocalSpeedVault during VDR restore

Technology carried forward from BMR implementation

Benefit: Improved RTO where LSV allows VDR to work at LAN speeds vs WAN speeds *This Service requires the use of USDV Software and Storage Services.*

***NOTE: To enable this Service you MUST backup your entire C drive, System State, ALL data files AND any other drives that contain needed programs or data files!**

Bare Metal Recovery / Virtual Disaster Recovery Enhancements

Support for Systems w/ EFI Bios

Support for Volumes w/ GPT Partitions

Benefit: Larger selection of Modern Windows Systems become eligible for Disaster Recovery with VDR & BMR technology

Versatile, innovative and deployable

Easy VM Restore for VMware

Backup Manager now preserves/ protects the VM system configuration during backup

Enables a direct restore to an existing or alternate VMware Host

Benefit: Improves recoverability and reduces mistakes by automating and replacing what used to be manual steps to restore a VM.

Hyper-V Granular Volume Selection

Ability to exclude individual .VHDs / volumes from backup or restore

Benefit: Granular selection saves time and money by allowing VM protection with reduced processing, shorter backup and restore times, reduced bandwidth utilization, smaller backup selection sizes and reduces cloud storage usage.



Scale-able High Performance

Skip Files During Restore

Option to ignore/ skip processing of files if they already exist

Available for Files system, Network shares, MS SQL & MS SharePoint plug-ins

Technology expanded from initial VDR/ BMR

Benefit: Better RTO by significantly reducing processing time, CPU overhead and recovery time when a large number of selected files are unchanged

Multi-threaded Restore

Minimum of 4 by default

Configurable settings on the local Backup Manager and remotely via the CMC

Available for all plugin restores from the Backup Manager as well as VDR and BMR

Benefit: Better RTO through parallel processing of restore operations and improved restore performance when sufficient bandwidth and system resources are available



Easy for you and your users

Backup Coach®™

2 Engines - Collection Engine & Communication Engine

#1- Identify common symptoms or errors and report back

Top issues are researched and KB articles written

#2 Future instances of popular errors get proactive communication with recommended steps to resolve

At Launch, we will have both Engines and a small list of top articles

Additional articles generated and released as needed over time

Separate from support KB system today, may be integrated in the future

Benefit: Reduced support calls, proactive patches and platform updates, improved visibility into problem areas, stronger knowledge base, higher backup success rates, happier partners and customers.

Autotask Integration

Enhancement to add the ability to choose between used storage and selected size



Easy deployment, larger customer more profitable

Remote Client Discovery & Deployment Benefits:

- Reduces deployment times for new customers
- Reduces the number of onsite visits
- Reduces dependencies on third party tools
- Ensures keys systems don't go unprotected
- Automates the discovery of systems at client locations
- Deploys the Backup Manager to one or more systems with just a few clicks

*Windows Environments Only

Remote Client Discovery & Deployment Process:

1. Select or create a new device in the CMC
2. Install first Backup Manager in the subnet using existing methods (onsite access, self-install, remote access, etc.)
3. From the CMC select a system to begin scanning the local subnet using provided credentials
4. Cancel scanning of current subnet for unprotected systems
5. Select one or more discovered systems and push deployment
6. Monitor the CMC for status updates

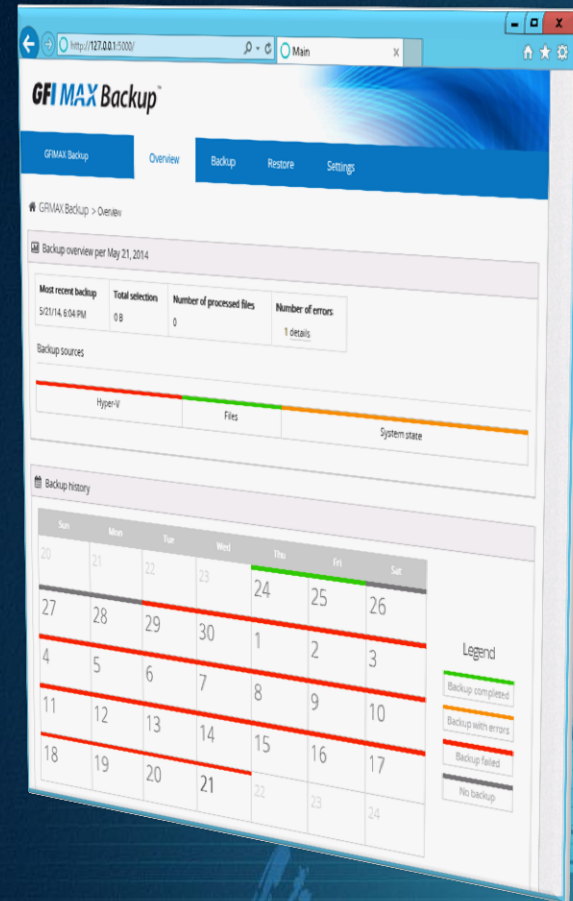


Usability and Manageability

HTML-Based Backup Manager

- Installable software client for
 - Windows, OS X & Linux Support
- Displays in the default browser
 - IE, Chrome, Firefox, Safari, etc.
- Simplified Branding
- Maintains core functionality
- Cleaner look & feel w/ Improved Usability
- Remote Launch from 14.x CMC
- Access from local network browser
- New Calendar view of Backup history

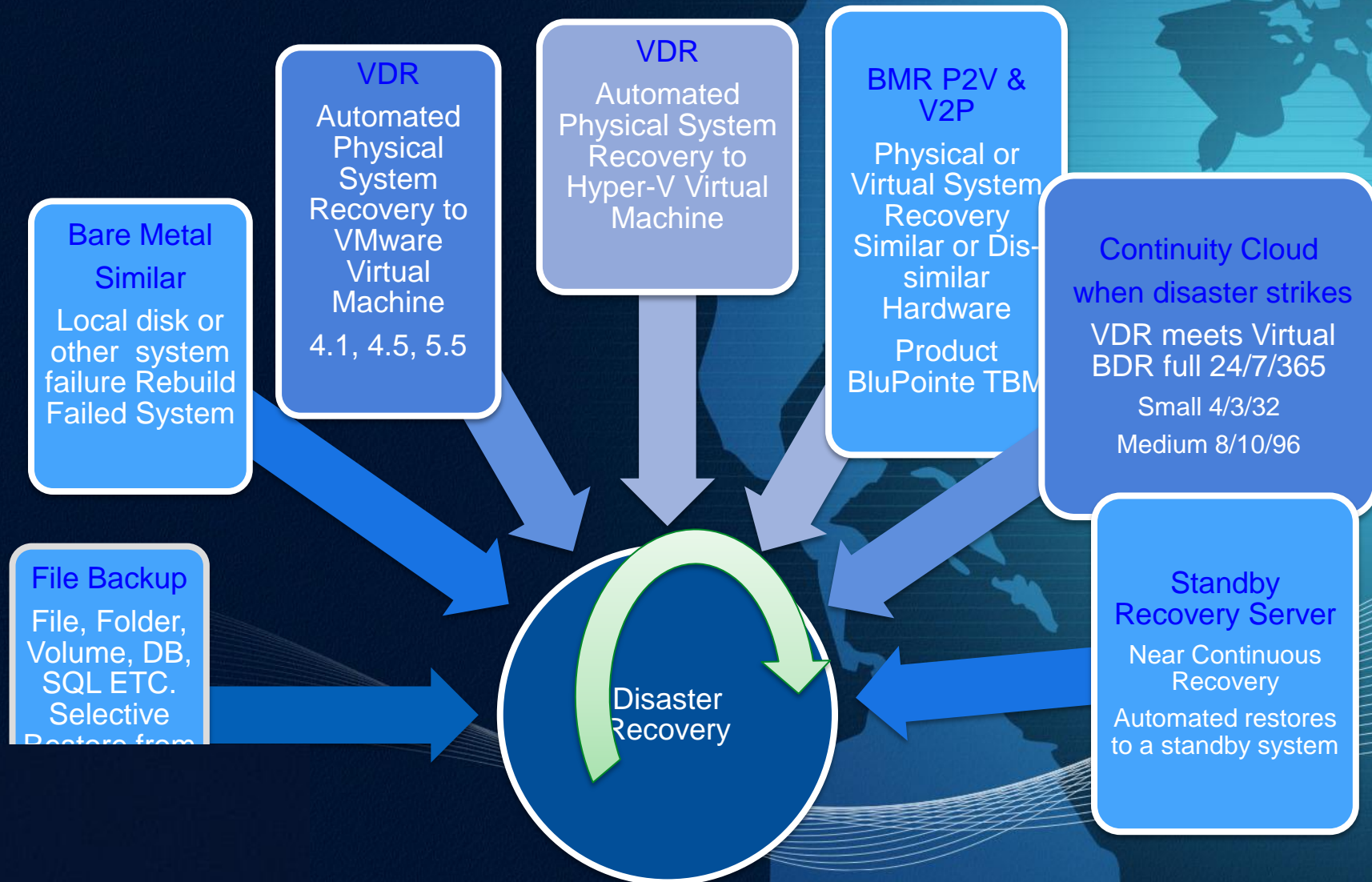
*Builds the platform for ongoing improvements to usability, alerting, reporting, communication, connectivity and responsiveness



Advanced Recovery Options



Single product for you and your customer.
Many opportunities to protect your customer,
many opportunities to advance your customer
and your relationship.



VDR

VDR is capable of recovering the following Windows Operating Systems:

- Windows Vista
- Windows 7
- Windows 8 / Windows 8.1
- Windows Server 2008 / Windows 2008 R2
- Windows Server 2012 / Windows 2012 R2

VDR is capable of restoring to the following targets:

- VMware ESXi 4.1 (Paid Version, Not FREE ESXi)
- VMware vSphere 5.0 / 5.5 (Paid Version, Not FREE ESXi)
- An offline *.VMDK file which can be mounted by VMware Workstation / VMware Player
- Microsoft Hyper-V compatible *.VHD file



Bare Metal Recovery

TBM (P2P, P2V or V2P) Bare Metal Recovery (BMR) allows for recovery of physical Windows systems to similar/like hardware or dissimilar

You must backup Minimum C:\ Drive and System State in order to do a successful restore.

Note: US DataVault TruBareMetal supports the following operating systems

VDR is capable of recovering the following Windows Operating Systems: VMDK or VHD

- Windows Vista
- Windows 7
- Windows 8 / Windows 8.1
- Windows Server 2008 / Windows 2008 R2
- Windows Server 2012 / Windows 2012 R2



Hyper-V Cluster Shared Volumes (CSV)

US DataVault - The first to bring Hyper-V CSV support to Online / Hybrid Cloud Backup.

Failover Clustering and CSV enables Highly available or continuously available file share storage for applications such as Microsoft SQL Server and Hyper-V virtual machines.

CSV is becoming a standard deployment for applications needing High Availability

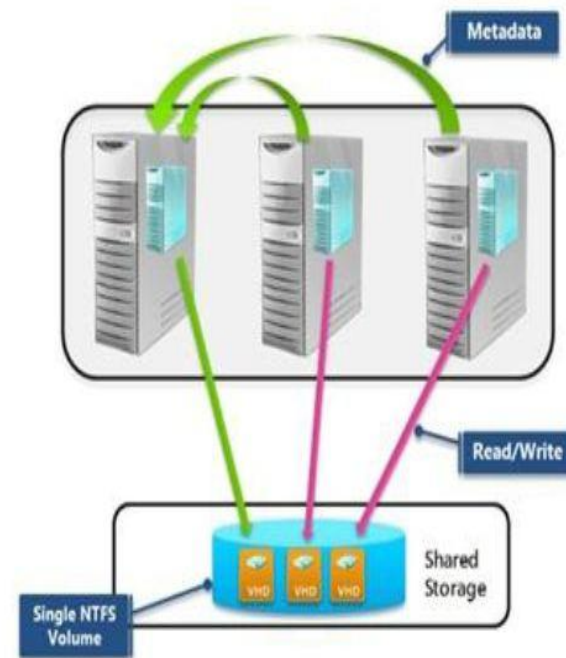


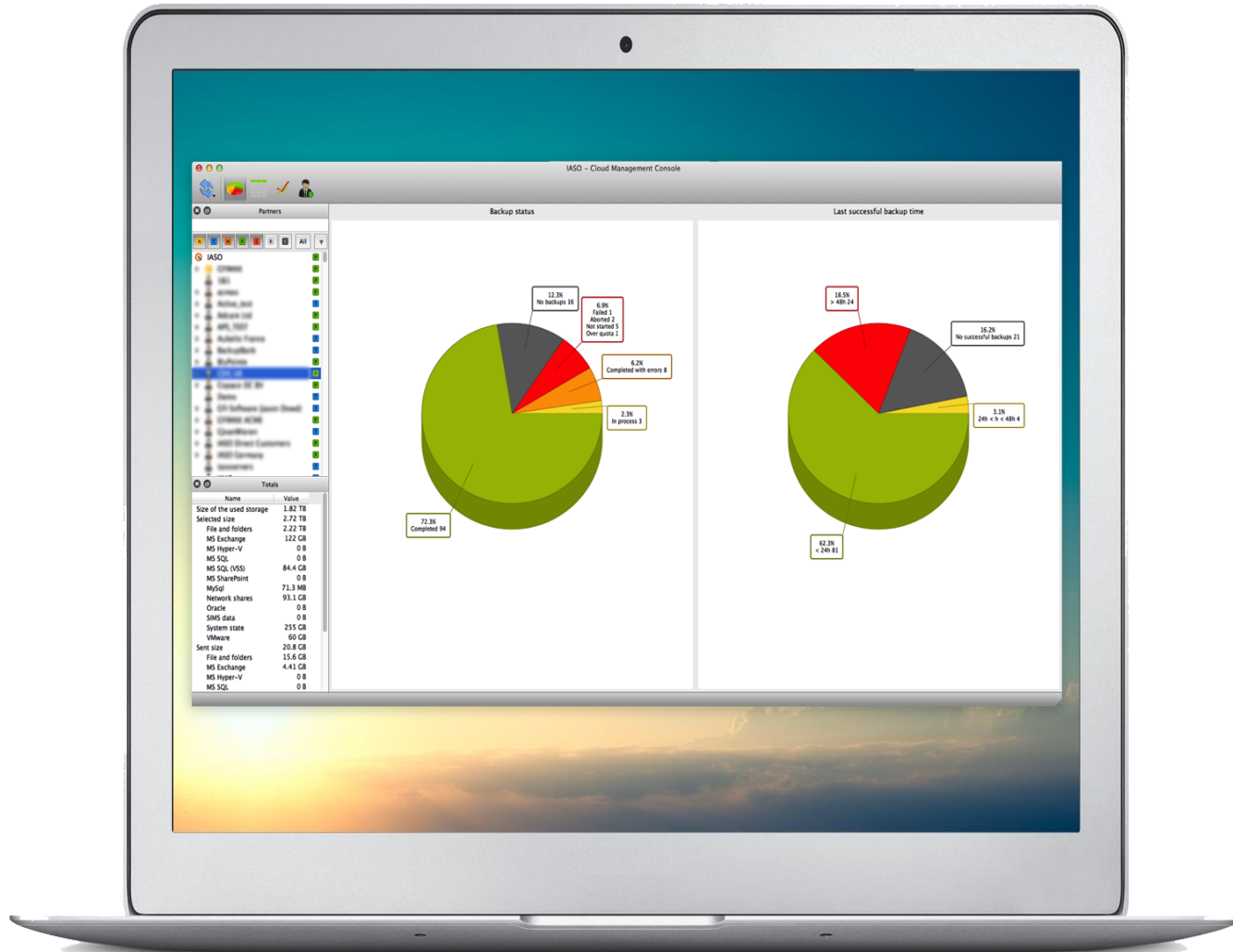
Figure 1 Cluster Shared Volumes



Live Monitoring



Centralized live monitoring



USDataVault Data Center Specifications



Data Center

Security

- 10 foot razor fence with 24/7/365 surveillance and patrols by armed security guards.
- State of the art data center ID system and security including video surveillance and recording.
- Multi-level identity verification, including biometric scanning, card keys, and badge authentication.
- Real-time IPS and multilevel firewalling, which comprehensively auto block sources of rejected traffic.

Power ($2N+1$)

- Multiple utility feeds from separate substations with diverse building entry
 - 11 generators providing a total of 7 MW of power, with in-ground fuel tanks to provide uninterrupted power for several days of outages. Fuel contracts guard against long-term outages.
- A+B feeds to each cabinet with A+B computing equipment, with each feed backed by independent N+1 power paths, including breakers, UPS systems, generators, and main feeds..



Data Center

Environmental Controls (**N+1**)

Environmentally friendly chilled water cooling, fed by redundant water sources (private well, city main), and powered by redundant pumps and paralleled 500-ton cooling towers.

Redundant Liebert Air systems providing consistent temperature and humidity range throughout the 70,000 square feet of datacenter space.

Continual environmental monitoring in each cabinet and through the data center, with threshold alarms monitored by the 24/7/365 NOC, providing fast resolution of anomalous conditions.

Network (**2N**)

Redundant Cisco BGP routing and switching infrastructure with cold spares on site. If equipment failure occurs, there is no interruption of service.

62 Gbit/sec Internet connectivity, delivered through multiple independent fiber rings and lines. Dual feeds of all aggregation routers ensure 100% uptime - some of the best in the business.

Avaya ANS BGP4 management system optimizing the routes on the network in real time, 7000 times per minute based upon trace route performance, to ensure low latency and high throughput.

6 backbone providers who are publicly peered with 12 providers including Earthlink.

Our current network consists of multiple 10 Gig or Gig links to Abovenet, Cogent, Level 3, nLayer, SAVVIS, TeliaSonera, XO, and the Atlanta Internet Exchange public peering point.



Data Center

- Avaya ANS BGP4 management system optimizing the routes on the network in real time, 7000 times per minute based upon trace route performance, to ensure low latency and high throughput.
- 6 backbone providers who are publicly peered with 12 providers including Earthlink. Our current network consists of multiple 10 Gig or Gig links to Abovenet, Cogent, Level 3, nLayer, SAVVIS, TeliaSonera, XO, and the Atlanta Internet Exchange public peering point.



US DataVault - Easily
Deployable, Extremely
Functional, Most
Reliable and Very
Affordable!

THANK YOU.





DataVault

We thank you for viewing our presentation and look forward to working with you!

**US DataVault, Inc.
Box 33
Pegram, TN 37143
615-933-USDV (8738)**

Skype: mhsusdv (email first)

**Follow us on Twitter: @usdv_mhs
AND Facebook: facebook.com/marc.shaffer.5**

Check out our Blog: <http://www.usdatavault.com/blog>

<http://www.usdatavault.com>

**sales@usdatavault.com customerService@usdatavault.com
techsupport@usdatavault.com**



DataVault

USDV Back-up Pro System 2 v14.1 Information

A LIST OF CLIENT SIDE FEATURES AND SUPPORTED PLATFORMS

Modified Mon, Sep 8, 2014 at 6:00 PM

<div></div>	supported	<div>-</div>	not supported	<div>~</div>	not tested	<div></div>	not supported by OS
-------------	-----------	--------------	---------------	--------------	------------	-------------	---------------------

Setup wizard	Windows									Mac OS (Intel)	GNU/Linu x	FreeBS D
	XP	Vista	7	8	Server					10.6 - 10.9	Any ₁	8-9
					2003	2008	2008 R2	SBS 2011	2012			
	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x64	x64	x86_64	x86_64	x86 & x86_64	x86 & x86_64
Setup Wizard	+	+	+	+	+	+	+	+	+	+		
Setup language	+	+	+	+	+	+	+	+	+	+		
Setup encryption method	+	+	+	+	+	+	+	+	+	+		
Setup encryption key	+	+	+	+	+	+	+	+	+	+		
Setup exclusion filters	+	+	+	+	+	+	+	+	+	+		
Setup simple schedule	+	+	+	+	+	+	+	+	+	+		
Setup e-mail address for Dashboards	+	+	+	+	+	+	+	+	+	+		

P.O. Box 33 • Pegram, Tennessee 37143

Backup	Windows									Mac OS (Intel)	GNU/Linux	FreeBSD
	XP	Vista	7	8	Server					10.6 - 10.9	Any ¹	8-9
					2003	2008	2008 R2	SBS 2011	2012			
	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x64	x64	x86_64	x86_64	x86 & x86_64	x86 & x86_64
Online backup	+	+	+	+	+	+	+	+	+	+	+	+
Offline backup	+	+	+	+	+	+	+	+	+	-	+	+
Delta backup	+	+	+	+	+	+	+	+	+	+	+	+
Automatic backup (on schedule)	+	+	+	+	+	+	+	+	+	+	+	+
Backup on shutdown	+	-	-	-	+	-	-	-	-			
System state backup	+	+	+	+	+	+	+	+	+			
MySQL 5.0 backup	+	+	+	+	+	+	+	+	+			
MySQL 5.1 backup	+	+	+	+	+	+	+	+	+		+	
MySQL 5.5 backup	+	+	+	+	+	+	+	+	+		+	
MySQL 5.6 backup	+	+	+	+	+	+	+	+	+		+	
MS SQL 2005 backup					+	+	+					
MS SQL 2008 backup				~	+	+	+	+	~			
MS SQL 2012 backup			~	+		+	+		+			
Exchange 2003 VSS backup					+	+	+		~			
Exchange 2007 VSS backup					+	+	+		~			
Exchange 2010 VSS backup					~	+	+	+	~			
Exchange 2013 VSS backup						~	~		+			

VMWare 4.1 backup	+	+	+	+	+	+	+	+	+			
VMWare 5.0 backup	+	+	+	+	+	+	+	+	+			
VMWare 5.1 backup	+	+	+	+	+	+	+	+	+			
VMWare 5.5 backup	+	+	+	+	+	+	+	+	+			
Hyper-V 2 backup						~	+					
Hyper-V 3 backup				~					+			
SIMS backup	~	~	~			~	+					
Backup of shared (Network) folders	+	+	+	+	+	+	+	+	+			
VSS SharePoint 2010 backup	+	+	+	+	+	+	+	+	+			
VSS SharePoint 2013 backup	+	+	+	+	+	+	+	+	+			
Oracle 11g backup	+	+	+	+	+	+	+	+	+			
Open files backup (VSS)	+	+	+	+	+	+	+	+	+			
Exclusion filters	+	+	+	+	+	+	+	+	+	+	+	+
Backup user rights (license-dependent)	+	+	+	+	+	+	+	+	+	+	+	+
Pre/post-backup actions	+	+	+	+	+	+	+	+	+	+	+	+
Encryption	+	+	+	+	+	+	+	+	+	+	+	+
Simple scheduling	+	+	+	+	+	+	+	+	+	+	+	+
Advanced scheduling (license-dependent)	+	+	+	+	+	+	+	+	+	+	+	+
Remote backup (from MC)	+	+	+	+	+	+	+	+	+	+	+	+
LSV	+	+	+	+	+	+	+	+	+	+	+	+

Restore	Windows									Mac OS (Intel)	GNU/Linux	FreeBSD
	XP	Vista	7	8	Server					10.6 - 10.9	Any ₁	8-9
					2003	2008	2008 R2	SBS 2011	2012			
	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x64	x64	x86_64	x86_64	x86 & x86_64	x86 & x86_64
Restore	+	+	+	+	+	+	+	+	+	+	+	+
Delta restore	+	+	+	+	+	+	+	+	+	+	+	+
System state restore	+	+	+	+	+	+	+	+				
MySQL 5.0 restore	+	+	+	+	+	+	+	+	+			
MySQL 5.1 restore	+	+	+	+	+	+	+	+	+		+	
MySQL 5.5 restore	+	+	+	+	+	+	+	+	+		+	
MySQL 5.6 restore	+	+	+	+	+	+	+	+	+		+	
MS SQL 2005 restore					+	+	+					
MS SQL 2008 restore				~	+	+	+	+	~			
MS SQL 2012 restore			~	+		+	+		+			
Exchange 2003 VSS restore					+	+	+		~			
Exchange 2007 VSS restore					+	+	+		~			
Exchange 2010 VSS restore					~	+	+	+	~			
Exchange 2013 VSS restore						~	~		+			
VMWare 4.1 restore	+	+	+	+	+	+	+	+	+			
VMWare 5.0 restore	+	+	+	+	+	+	+	+	+			
VMWare 5.1 restore	+	+	+	+	+	+	+	+	+			
VMWare 5.5 restore	+	+	+	+	+	+	+	+	+			
Hyper-V 2 restore						~	+					

Hyper-V 3 restore				~					+			
SIMS restore	~	~	~			~	+					
Restore of shared (Network) folders	+	+	+	+	+	+	+	+	+			
VSS SharePoint 2010 restore	+	+	+	+	+	+	+	+	+			
VSS SharePoint 2013 restore	+	+	+	+	+	+	+	+	+			
Oracle 11g restore	+	+	+	+	+	+	+	+	+			
Restore of selected files only	+	+	+	+	+	+	+	+	+	+	+	+
Restore to the original/alternative location	+	+	+	+	+	+	+	+	+	+	+	+
Selection of backup session for restore	+	+	+	+	+	+	+	+	+	+	+	+
VMware per files restore	+	+	+	+	+	+	+	+	+			
Restore on Desktop	+	+	+	+	+	+	+	+	+			

Updates	Windows									Mac OS (Intel)	GNU/Linux	FreeBSD
	XP	Vista	7	8	Server					10.6 - 10.9	Any ₁	8-9
					2003	2008	2008 R2	SBS 2011	2012			
	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x64	x64	x86_64	x86_64	x86 & x86_64	x86 & x86_64
Manually update	+	+	+	+	+	+	+	+	+	+	+	+
Auto-update	+	+	+	+	+	+	+	+	+	+	-	-

Technologies	Windows									Mac OS (Intel)	GNU/Linux	FreeBSD
	XP	Vista	7	8	Server					10.6 - 10.9	Any ₁	8-9
					2003	2008	2008 R2	SBS 2011	2012			
					x86 & x64	x86 & x64	x64	x64	x86_64	x86_64	x86 & x86_64	x86 & x86_64
De-duplication	+	+	+	+	+	+	+	+	+	+	+	+
Delta slicing	+	+	+	+	+	+	+	+	+	+	+	+
Directory hashing	+	+	+	+	+	+	+	+	+	+	+	+
Cabinets	+	+	+	+	+	+	+	+	+	+	+	+
FTP over SSL protocol usage	+	+	+	+	+	+	+	+	+	+	+	+

Other	Windows									Mac OS (Intel)	GNU/Linux	FreeBSD
	XP	Vista	7	8	Server					10.6 - 10.9	Any ₁	8-9
					2003	2008	2008 R2	SBS 2011	2012			
					x86 & x64	x86 & x64	x64	x64	x86_64	x86_64	x86 & x86_64	x86 & x86_64
GUI	+	+	+	+	+	+	+	+	+	+		
Management Console	+	+	+	+	+	+	+	+	+	+		
Visualization of backup/restore processes	+	+	+	+	+	+	+	+	+	+		
Software runs as a service	+	+	+	+	+	+	+	+	+	+		
Conveniently arranged tree-structure	+	+	+	+	+	+	+	+	+	+	+	+

Branding/Skinning	+	+	+	+	+	+	+	+	+		
Backup Register	+	+	+	+	+	+	+	+	+	+	+
Client driven cleaning	+	+	+	+	+	+	+	+	+	+	+
Archiving	+	+	+	+	+	+	+	+	+	+	+
Multi-lingual support	+	+	+	+	+	+	+	+	+	+	+
Deep branding	+	+	+	+	+	+	+	+	+	+	+
Remote management	+	+	+	+	+	+	+	+	+	+	+
Proxy support	+	+	+	+	+	+	+	+	+		
Status window	+	+	+	+	+	+	+	+	+		
Tray icon notifications	+	+	+	+	+	+	+	+	+		
Dynamic slicing	+	+	+	+	+	+	+	+	+	+	+
Limits functionality	+	+	+	+	+	+	+	+	+	+	+
Deep Brand-able Common Users	+	+	+	+	+	+	+	+	+	+	+
Connection State Viewer	+	+	+	+	+	+	+	+	+	+	+
Local cabinet disk cache	+	+	+	+	+	+	+	+	+	+	+
Local databases	+	+	+	+	+	+	+	+	+	+	+
UAC		+	+	+		+	+	+	+		
Search	+	+	+	+	+	+	+	+	+	+	+
Priority	+	+	+	+	+	+	+	+	+	+	+
WebDAV	+	+	+	+	+	+	+	+	+	+	+
Multiple connection to BackupFP	+	+	+	+	+	+	+	+	+	+	+
Virtual Drive for File System	+	+	+	~	+	+	+	~	~		
Virtual Drive for Exchange 2007 VSS				~	+	+	+	~	~		
Virtual Drive for Exchange 2010 VSS				~	~	+	+	~	~		
Remote installation	+	+	+	+	+	+	+	+	+		

Disaster Recovery	Windows								Mac OS (Intel)	GNU/Linux	FreeBSD
	XP	Vista	7	8	Server				10.6 - 10.9	Any ¹	8-9
					2003	2008	2008 R2	SBS 2011			
	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x86 & x64	x64	x64	x86_64	x86_64	x86 & x86_64
Virtual Disaster Recovery	-	+	+	+	-	+	+	+	+	-	-
Bare Metal Restore	-	+	+	+	-	+	+	+	+	-	-

¹ **NOTE:** Although the software runs practically on any GNU/Linux x86 and x86_64/amd64 distribution with GLIBC 2.3.2 or higher (with NPTL enabled), officially supported are: CentOS5, CentOS6, Debian5, Debian6, OpenSUSE11, OpenSUSE12.

2 NOTE: USDV provides 24x7x365 telephone and email support to all Clients and Salespeople.



DataVault

Why do business with **USDV**? A question we get asked every day... Aside from our long time policy of NOT being undersold by a competitor ("anyone who sells at our level of quality, functionality, redundancy and service"), I think you will find several other highly competitive reasons below.

Almost everything here comes directly off our literature and/or Web Site.

USDV System 2 is Fast, Reliable and VERY Secure. And, is VERY affordably priced!

USDV has been providing constantly accessible (average 99.98% up time), highly secure data space for over 15 years with not a single breach or loss of Client data. And we have helped hundreds of Clients quickly recover from data loss or disaster.

Everything you need to do and all of the tools you need are contained within our **USDV Backup Pro** software, or via our proprietary on-line Client Control Panel.

Should a Client have more data than their connection will bear, they can use our software to do a local backup to an external drive, then ship it to us for import. The cost for that is \$100 per hour and generally takes no more than an hour or two to accomplish depending on volume. The same can be done for data recovery if using our tools and recovering on-line is not possible.

USDV provides 24x7 email tech support access as well as live on-line tech chat M-F from 9-5 Eastern time to all our Clients. And we have a strong Help Desk Solution powered by Cayzu! Commercial Clients ALWAYS have 24x7x365 phone support.

Additionally, anytime a Client has an urgent problem all they need to do is CALL US, **anytime**. It is our mandate to be there for them.

USDV provides a FREE, redundant copy of the data at a 2nd remote data center.

All **USDV** data centers are high security, multiply redundant for power and connection, and manned 24x7.

P.O. Box 33 • Pegram, Tennessee 37143

ALL Client data is compressed and encrypted BEFORE it leaves their facilities. Clients have encryption choices from 256 AES up to true 448 Blowfish.

NO USDV personnel have access to Client data. We do not have the encryption key.

USDV is fully compliant with all Federal laws and regulations concerning data security. As well as all industry and insurance codes, including Safe Harbor.

There are NEVER any hidden or unexpected costs with **USDV**.

In over 15 years of operation, **USDV** has never lost or exposed Client data, NOT 1 BYTE.

Let us know how we can be of service...

US DataVault, Inc.

Marc H. Shaffer
CEO

Mail: Box 33, Nashville, TN 37202-0033

Email: mhs@usdatavault.com

URL: <http://www.usdatavault.com>

Telephone:

Office: (615) 933-USDV

Direct: (615) 414-1513

Fax: (615) 523-4898



At US DataVault, our Business is KEEPING YOU in Business!

P.O. Box 33 • Pegram, Tennessee 37143