assured
data protection

Whitepaper

Advantages

of Moving Data Backup and DR to a Managed Services Model

assured data protection

Whitepaper

Advantages of Moving Data Backup and Disaster Recovery to a Managed Services Model

INTRODUCTION:

Most IT Directors recognize that their current backup and disaster recovery solution lacks true reliability, takes too much time and requires increasing numbers of staff hours each day to maintain. On top of that, many express doubt that restores would even work in a disaster situation.

You know you need to make changes to protect your company's data, but the options seem endless and you are not sure which choice best suits your business.

If these concerns resonate with you, you are not alone. This white paper will provide information about the key advantages of a Managed Services approach to data backup and disaster recovery for organizations of any size.

ABOUT ASSURED DATA PROTECTION

Assured Data Protection eliminates the complexity, expense and management of in-house backup, recovery and data protection by offering it as a managed service. We combine award-winning Rubrik software with our technical and operational expertise which includes more than 100 collective years of industry experience. We tailor our solutions to meet the individual business needs of mid-market enterprises making them affordable and achievable, from on-premise private clouds to hybrid cloud approaches. Visit: www.assured-dp.com for more information.

CHAPTER 1: BACKUP AS A SERVICE

How does Backup as a Service work?

There are various levels of Backup as a Service. These range from basic hardware offerings through "Rolls Royce" solutions that deliver entire environments featuring all backups, completely monitored and handled. This level of service includes having the individual file restores taken so your team no longer has to perform these.

While multiple benefits exist for doing data Backup as a Service (BaaS), the overarching advantage is the ability to hand this critical IT activity over to outside experts to implement and manage, allowing you to focus on other important aspects of your role.

Rob Mackle, Director and Co-Founder of Assured Data Protection, explains why there is such a need for automation and systems that work quickly in today's environment:

> "Many IT teams are stretched in their duties as a result of staff reduction or overall resource constraints. Formerly, most teams had a dedicated backup admin in place but that has become very uncommon. When backup can be outsourced to a managed service provider (MSP), it frees up staff time, ensures backup events run smoothly and ensures the documentation needed for audit purposes is complete."

The main benefits of BaaS include:

- A consultative and tailored approach to the design and installation of your solution.
- A pay-as-you-grow solution which is flexible, scalable and affordable.
- Expert support for all your daily backup and recovery requirements.
- A manageable all-inclusive cost, based on your data size.

Ian Thompson, Assured Data Protection's UK Head of Data Services, emphasizes the financial attraction of Backup as a Service:

> "Backup as a Service can be as simple as providing customers with an OpEx model to purchase. It can be viewed as a financing arrangement."

What are the costs associated with BaaS?

Even with the monthly costs associated with a managed service provider (MSP), utilizing Backup as a Service typically delivers a total cost of ownership (TCO) savings of up to 50% by:

- Eliminating the need for tapes, tape drives and the costs of storing backup tapes offsite.
- Reducing backup software and hardware costs.
- Savings on backup management time.
- Reducing your data center footprint as you will need less space for storage.

Who would BaaS best suit?

The fast growth of data sources and real-time communication channels have forced IT professionals to look beyond conventional backup methods.

The Backup as a Service model suits a wide range of enterprises from large organizations to smaller companies with only 1-2 Terabytes (TBs) of data.

Key business reasons that enterprises choose Backup as a Service include:

- **Financial** – Backup as a Service offers a more affordable option with an Opex pay-as-you-grow model.
- **Positioning** – if your competitors have modernized their data protection solutions, you may want to position yourself on an even (or superior) footing to them.
- **Convenience** – some businesses want to outsource their entire backup process and never see it again. BaaS can make this possible.

How long does it take to get up and running?

BaaS has a simple setup, makes use of automated elements to speed up the process and offers reliability.

Depending on the vendor solution, it may take a few hours to install and only between 1-2 weeks to get fully seeded and operational. The size of your environment, the number of existing backups to be migrated and the specificity of backup times determines the true timeframe.

How does Backup as a Service save time?

Time ranks as one of the largest currencies for most businesses. Companies choosing Backup as a Service seek ways to expand employee bandwidth and productivity without the distractions and irritation of constantly monitoring backups. Here are three of the biggest advantages:

- Switching to automated backup policies allows backup to occur behind the scenes instead of at the forefront of everyday tasks, saving time for IT managers and their teams.
- Eliminating the need for managing backup capacity and the rescheduling of jobs to try and run efficiently with the tape becomes a thing of the past.
- Removing the time-sapping nature of regular manual backups which have to be revisited once set.

CHAPTER 2: FULLY-MANAGED DATA BACKUP AND DATA RECOVERY SERVICE

What should a Fully Managed Service offer?

Businesses seeking a comprehensive up-to-date, thorough and secure data-recovery approach for their data protection adopt a Fully Managed service. It unifies backup, recovery, analytics and compliance into one high-end solution.

For businesses that recognize that their current data-protection solutions lack rigor, Rob Mackle explains they are not alone:

> "Technical problems cause the biggest concern for IT departments. Simple things like backup windows and timeframes to complete backups can create anxiety. If underlying technology or the environment is not up to standard, backups will not scale properly. This is where a Fully Managed Service can really make the biggest difference."

Other features of a Fully Managed Service include:

- Obtaining a solution tailored to your specific business requirements.
- Gaining an MSP that takes full ownership of the backup and restores.
- Ensuring backup monitoring occurs which will help prevent failures.
- Communicating with MSP experts in the event of failures or issues.
- Acquiring continuous, around the clock support.

What are the costs and savings associated with a Fully Managed Service?

Significant TCO savings can be gained through reduction of hardware, software and management time. This makes it a difficult option to ignore for businesses who want both a financially viable and all-encompassing solution.

You can protect any number of hosts or virtual machines (VMs) while only paying for the protected data size or level of service that you need.

A Fully Managed Service can be highly customized with cost options tailored to your business and budget, too. It should be available as either a Capex or an Opex model (usually Opex) which makes it an affordable and achievable option for organizations of all sizes.

What are the advantages of a Fully Managed Service?

There are multiple reasons to choose a Fully Managed Service. Investment in a data protection solution is something you can't afford to get wrong so MSP can offer added peace of mind. They will already have a good working relationship with the vendor, plus they will have solid technical knowledge and expertise of that platform which saves you training your team in order to deploy a new solution.

Who would a Fully Managed Service best suit?

Due to the comprehensive nature of this service, it tends to be businesses at the top end with larger budgets and the most at stake if there was an issue, who choose this option.

These are companies where backup is more closely monitored – this could be for financial or confidentiality reasons.

Information Age explains why many large businesses are turning to managed service providers (MSPs):

> "Technology grows in complexity by the day, internal IT departments with limited resources struggle to keep up with it all. Good MSPs can provide a steady level of support to meet challenging requirements...MSPs increase efficiency in that they can offer working dynamics that internal teams may not be able to do, for example, 24×7 coverage."

How long does a Fully Managed Service take to get up and running?

A Fully Managed Service involves continuous refinement rather than a start and finish time.

After deployment, it should be up and running in 2-3 weeks. Changes to servers, backups, or SLAs will need constant monitoring but your MSP will handle the day-to-day to keep things updated and running smoothly.

The timeframe depends largely on how long you need to keep your data and how fast your environments change. Every business will have unique requirements that impact the timeline.

How does a Fully Managed Service differ from legacy solutions?

The biggest difference: all your data-protection solutions become centrally managed. That means no more confusion about who is running which backups or which providers are responsible for which aspects of your data protection. Everything is maintained in one place.

In addition, you receive the support, interaction and guidance whenever you need it, all the time.

CHAPTER 3: DISASTER RECOVERY AS A SERVICE

How does Disaster Recovery as a Service Work?

Disaster Recovery as a Service (DRaaS) further enhances BaaS by providing the ability to replicate all the critical company information offsite to a disaster-recovery location. In the event of a significant IT failure, servers, applications and data can be brought online rapidly to allow the business to continue operating with minimum disruption.

It is fully managed, flexible and scalable. It enables an enterprise to have its systems fully recovered by an expert third party at a geographically independent site, eliminating the need to involve staff and resources.

What are the costs associated with Disaster Recovery as a Service (DRaaS)?

Obtaining high-performance DR at a fraction of the cost of legacy solutions makes this a highly attractive option for companies from a budget standpoint

In contrast, running DR in-house carries significant upfront investment costs including having to upskill and train existing staff or hire new staff – plus the extra time needed to manage, maintain and test.

Not only is Disaster Recovery as a Service cost effective, but sending your on-premise data to the cloud is quick and easy, further improving the productivity of your team.

What are the Advantages of DRaaS?

- Rapid recovery with minimal input from your IT staff in a time of crisis.
- Experienced third party to help manage the DR function.
- Reliability because data is stored on disc with error checking and parity.

Ian Thompson explains why DRaaS offers such a lifeline for many businesses:

> "Having third party experts close at hand in the event of a disaster, such as your building becoming inaccessible or the loss of primary servers, is an enormous relief."

What Size Company does DRaaS benefit most?

It suits many organizations including:

- Small to medium enterprises (SMEs) or large companies within their own environment.
- Enterprises with a single site where all technology resides.
- Businesses with a single or a small IT department.

How long does DRaaS take to get up and running?

The average time for Disaster Recovery as a Service full setup is approximately six weeks. The typical timeline includes:

- Initial deployment
- Backup configuration
- Initial backups during weeks 1-2
- Backups are replicated over weeks 3-4
- The disaster recovery test is scheduled over weeks 5-6

How reliable is DRaaS?

DRaaS must be reliable: it is the insurance policy if the worst happens. If you currently lack confidence in your approach, examine your existing technology to perfect that recovery or consider alternatives.

A good DRaaS MSP will not only allow you to test the recovery platform, but should actively encourage it. Only by testing the process end-to-end can you obtain assurance of reliability.

An Information Age article reveals worrying statistics on companies without a reliable disaster recovery solution in place:

> "Only 29% [of participants] said they could get hardware to replace servers... and just 29% said they could recover to the cloud, 54% admitted they couldn't – 17% said they didn't know...What's clear from our research is that, for many companies, disaster recovery is shelfware, set up once and then rarely, if ever, tested or thought of again."

How does DRaaS differ from traditional solutions?

- Abolishes need for additional hardware, software or a secondary site.
- A proven process and defined architecture facilitates recovery.
- Offers native access to the data without waiting for lengthy restorations since it is already on disks in the DR site.

Other Considerations for DRaaS:

If you regularly change your servers, the layout of your data or the way your products work, you will have to keep your DraaS MSP regularly informed so they can best update your systems and keep you fully protected.

Companies with particularly sensitive data such as government agencies or financial institutions might not want their data being recovered in a third-party data center for security reasons. In these situations, a full private cloud BaaS and DraaS solution will ensure compliance.

CHAPTER 4: VIRTUAL DESKTOP AS A SERVICE (VDAAS)

What is Virtual Desktop as a Service?

Virtual Desktop as a Service (VDaaS) provides a "desktop" in the cloud for your workforce so they can access email and their software applications from anywhere. It enables employees to continue working using their own computers, tablets and mobile devices and get back online after a major outage. It complements DRaaS as it provides users with a fast and flexible way to get back to business across the internet from any device.

What are the costs associated with Virtual Desktop as a Service?

This service acts as an add-on feature for those already using a DRaaS solution. It usually requires an upfront commitment to the service and an affordable monthly fee assessed on a per desktop basis.

What are the advantages of virtual desktops?

- Delivering a work environment from any device, anywhere, with an internet connection.
- Obtaining secure connectivity to all servers and applications during a DR.
- Providing users with a familiar experience.

Who would Virtual Desktop as a Service best suit?

Virtual desktops are a great solution to aid Business Continuity and would suit:

- Organizations lacking contingency plans for hosting users in an alternative local office, if the primary office is unavailable.
- Companies using VDI at present and want to extend this during DR.
- Enterprises already using DRaaS.

How long do virtual desktops take to get up and running?

Virtual desktops should be ready to use as soon as servers are restored, typically within three hours. The provision of a virtual desktop happens in parallel with server recovery and setting up the rest of the environment. Employees can get their emails, carry on with their work and perform their jobs without issue in a matter of a few hours.

How does it differ from traditional solutions?

Five or ten years ago, if computers went down, employees likely had manual tasks they could do until their desktops came back online. In today's digital age, that is not the case. Work performance without desktop access would now be nearly impossible.

Virtual Desktop as a Service means having a provision in place for enabling your workforce to continue as usual in a fast turnaround.

CHAPTER 5: CONSIDERATIONS FOR WHOLE SERVER RECOVERY

In an ideal world, every server would be virtualized, modern and therefore predictable to backup and recovery. In the real world, however, legacy systems can cause delays.

Your BaaS solution, and where applicable, your DRaaS solution must be able to handle all aspects of your data center recovery. When undergoing a serious outage, legacy systems can stress the recovery process and lengthen the time to get your workforce back online.

Common issues experienced with whole-server recoveries

There are recurring issues that many companies experience when attempting a whole-server recovery. Some of these may sound familiar:

- Mismatched physical hardware, causing driver conflicts and issues booting the Operating System.
- Older version of VM hardware or disk types, unsupported on recovery systems.
- Lengthy recovery times waiting for large VMs to restore.
- Attempts to recover older unsupported OS on modern hypervisors.
- Recovering sub-standard, poorly performing hardware which lengthens recovery times and frustrates end users with slow data access.
- Failure to perform a full recovery test to prove successful backups, and document end-to-end recovery procedures ahead of a real invocation.

Best Practices for Whole Server Recoveries

There are a range of ways to avoid some of the most problematic issues during whole-server recoveries. These include:

- Performing at least one recovery test for each server to prove you have a process and doing so at least one or twice a year, or after any major server changes.
- Ensuring all backups are full backups so recovery does not require multiple incremental recoveries which may fail.
- Planning to conduct backups offsite as soon as possible after completion, preferably at your DR location.
- Scheduling backups to run 7 days a week, including holidays.
- Designing the DR equipment to handle the Input/Output of the users, but also the IO of the recovery operation itself, within acceptable timeframes.
- Considering using an expert DRaaS provider if your business has recovery requirements that exceed your current capacity or budget.

No matter what your company size, budget or security needs, there is a new solution for you. Whichever you decide to pursue, you've made a step towards exploring your options, so the hardest part is already done.

Your company's data protection should be at the forefront of your IT department's priority list. We hope this white paper acts as a useful tool.