UNIFIED DATA PROTECTION FOR LONG-TERM SURVIVAL

Organizations know—whether or not they learned it the hard way—that creating backups of their most important data assets keeps it safe from disasters and accidental deletion. They have done backups for decades with little to no changes. However, their backup data stores continue to grow as they use a more diverse set of data to make business decisions and digitize larger parts of the business processes and supporting data.

Today, applications and data are hyper-fragmented across multiple clouds, data centers, countries, and continents. The inevitable parallel result of this fragmentation is often a creeping change to their traditional way of doing backups, making it an extremely complex and a costly burden for organizations to assure timely access to the backup data, putting survival of the business at risk.

Organizations that want to seriously participate in the new digital era will find out that they can’t continue cobbling together makeshift data protection solutions from different point-product vendors. Adding more infrastructure to deal with the scale and performance challenges is clearly not sustainable in the long-term.

What these organizations require is a unified data backup solution that covers all their heterogeneous environments and that integrates seamlessly with the leading enterprise cloud platforms out there.

ESG Research surveyed how organizations leverage cloud (see Figure 1) and found that data protection efforts (specifically backup, archiving, and disaster recovery) sit at the top of the cloud use-case list right now.

TOP FIVE CLOUD INFRASTRUCTURE USE CASES

For which of the following purposes does/did your organization use cloud infrastructure services? (Percent of respondents, N=319, multiple responses accepted)

- Data backup and archive: 46%
- Disaster recovery: 36%
- Run internal production applications: 31%
- Primary storage for files: 30%
- Run internally/externally facing web servers: 30%

Figure 1: Top Five Cloud Infrastructure Use Cases. Source: Enterprise Strategy Group, 2016.

CONSIDERATIONS WHEN USING CLOUD FOR DATA PROTECTION

Leveraging cloud-based storage to augment on-premises data protection is growing in popularity. In fact, ESG Research says that 25% of organizations today use cloud-based capacity to store backup data remotely, with another 23% intending to do so within the next 12 months.

The ability to store data remotely on cloud-based storage for disaster recovery, for example as an alternative for traditional tape, is a top driver. It not only can improve disaster recovery preparedness, but it can also save an organization time and money in restoring operations.

Most organizations that are adding cloud-based storage to existing data protection prefer one or sometimes a combination of the following 2 ways:

- **Disk to Disk to Cloud (D2D2C)**—Data is initially backed up to on-premises disk storage, and a copy is then sent to a cloud service provider
- **Disk to Cloud (D2C)**—Data is backed up over the WAN to a cloud service provider (no on-premises storage of the backup data)

Both have their pros and cons. The main deciding factor between them usually centers on the organization’s recovery requirements. Specifically, the service level objectives that IT teams have with internal business units and external customers sometimes demand a faster, more agile recovery capability than what a pure-cloud (i.e., D2C) arrangement can typically accommodate. Therefore, the need to recover data locally tends to drive the decision to D2D2C, because for many organizations performance (aka recovery speed) is of utmost importance when it comes to recovering their data.

STOP BACKING UP DATA BLINDLY

Another critical consideration when using cloud for data protection involves having a clearly defined backup data lifecycle. This is often an overlooked element, but crucial to get right. Organizations must match the backup policies to the data they protect. By understanding data and its value as an asset or liability, organizations can properly assign backup methodologies and policies to protect and store their data as it ages. For example, deep knowledge of the true composition of the data an organization is storing, empowers backup administrators and application owners to:

- Choose different backup methods for different types of data based on change rates and recovery requirements.
- Use deduplication and compression when and where it makes the most sense.
- Set up different backup retention policies for different recovery needs.
- Adopt archiving, instead of backup, for long-term data retention.
- Confidently dispose data that is no longer necessary to keep.

“When organizations cannot effectively identify their critical data amongst the junk, they waste money, time and protection effort on an environment where 41% of the data is of questionable value.”

—The Databerg Report, Veritas, 2015
Without this understanding, data may be overprotected or perpetually retained to address worst-case fears of data loss, drastically driving up storage and management costs.

THE REAL COST OF DATA PROTECTION

The real cost of data protection is not just the cost of the raw storage capacity. It also includes backup infrastructure software and hardware, maintenance contracts, remote vaulting services, and administrative staff/time and operational processes. These elements (regardless whether tape, disk or cloud is used) and associated cost models dramatically vary from one organization to another, which makes delivering a universal cost calculation a nearly impossible task.

One cost advantage of tape that we must take into account is that many organizations have made substantial investments over the years in tape libraries and drives. These investments typically last seven to ten years without the need to refresh. Some may be halfway their depreciation cycle, which is probably one of the reasons why tape is still used in about 60% of the backup deployments today. Most organizations have a good idea of the cost of their tape infrastructure. However, they are often unsure of the cost of using cloud for data backup. While organizations won’t face high upfront capital outlay, there are variable elements associated with cloud storage usage, which can make it seem harder to predict recurring cost. However, Table 1 lists the major cost factors with their associated considerations.

<table>
<thead>
<tr>
<th></th>
<th>Tape</th>
<th>Disk</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital outlay</td>
<td>Medium</td>
<td>High</td>
<td>None</td>
</tr>
<tr>
<td>Capacity cost</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Shipping &amp; Logistics</td>
<td>Medium</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Networking cost</td>
<td>None</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Personnel cost</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Recovery cost</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

Table 1: Cost of Backup

Taking in to account the above table—although being far from a comprehensive analysis—it should come as no surprise that cloud-based storage is growing popularity these days as a remote backup target beyond on-premised disk-based recovery, often at the expense of tape—especially where investments in tape are fully depreciated and due for refresh.

THE VERITAS APPROACH: UNIFIED DATA PROTECTION FOR THE CLOUD

Veritas™ Unified Data Protection delivers the flexibility to meet all your cloud backup needs. Supplementing it with cloud, is one of the most effective ways to advance your data protection strategy and probably the least invasive too, because integrating cloud storage from our growing list of supported cloud providers, is a seamless experience. Assigning the accurate backup policies to protect and store your data is key to your strategy. Data may be overprotected or perpetually retained, which drive up storage and management costs. So before you start to make key decisions about your cloud data protection strategy, you must be made to ensure you get the best possible outcome.

Choose the cloud service provider that best fit your unique requirements

In NetBackup™, you can choose from a range of NetBackup fully tested and certified integrated cloud connectors—AWS S3, Microsoft® Azure, Microsoft Exchange Office365, Google Cloud Platform Storage, Oracle Cloud Platform, Oracle Database Server, Box, IBM Bluemix, Hitachi, and SwiftStack.
Rapid deduplication of data from the data center to the cloud

Veritas NetBackup™ CloudCatalyst fits into existing NetBackup environments to help automate a customer’s path to multi-cloud environments. Optimize data reduction with NetBackup CloudCatalyst and speed end-to-end deduplication up to an average of four times faster than alternative solutions before sending data to the private or public cloud.1 Dramatically reduce time, cost and network bandwidth for cloud storage. Fast recovery of data can also be performed directly from NetBackup CloudCatalyst to the NetBackup Client. The new deduplication technology is available as a build-your-own (BYO) media server configuration powered by NetBackup 8.1 software, or as a prebuilt, all-in-one NetBackup™ 5240 Appliance configuration.

Bring visibility to your data protection

Use Veritas™ Information Map to get a clear line of sight into your environment and the nature of the data being stored, helping you to accurately assess your complete data inventory and expose hidden vulnerabilities and costs. The immersive, visual experience of Information Map is now enhanced with connectors for 23 new data sources for both on-premises and cloud-based data storage repositories. With better visibility, customers will gain actionable insights and help ensure adherence to compliance regulations, such as HIPPA or the European Union’s forthcoming General Data Protection Regulation (GDPR).

Always maintain an on-premises disk-based backup tier, with short retention for fast recovery

Veritas NetBackup Appliances deliver a turnkey replacement for your build-your-own data protection infrastructure, while also functioning as your hub to the cloud storage. This delivers you the advantage of purpose-build, performance-optimized local storage for your critical data backups close to your production applications for immediate restore, while your NetBackup policies automatically move less critical data securely to your cloud storage destination for disaster recovery without compromising timely access.

Extend unified data protection to your cloud-based applications

The presumption that more organizations eventually move applications to the cloud makes a case for hosting NetBackup servers in the cloud as well. Easily deploy NetBackup in AWS EC2 with - the NetBackup Amazon AMI. It is a smart way to extend your enterprise data protection to your cloud-based applications without the need for new tools or processes. One backup console to manages and governs your backups across all your clouds, and local virtual-bare-metal servers.

1. Veritas internal benchmark testing that compared NetBackup CloudCatalyst with competitive backup software
Improve disaster recovery readiness

Replication of your on-premises virtual and bare-metal server images to cloud storage, simply using NetBackup™ Auto Image Replication, can turn your cloud NetBackup infrastructure into a disaster recovery strategy quickly and at a fraction of the cost of dedicated disaster recovery implementations.

WHY VERITAS

Veritas is trusted today to provide enterprise data management to organizations of all sizes, including 86 percent of global Fortune 500 companies. Veritas is unique in providing solutions that are software-based, vendor-agnostic, and infrastructure independent, uniquely focused on the value of information rather than the underlying environment.

Organizations today need to manage their data as a critical asset, with solutions that reliably protect the right data, help ensure resiliency and on-demand access from anywhere, and reduce the risks and costs of storing their ever-increasing amounts of data throughout the globe.

The ‘always on’ nature of digital business also demands the removal of the artificial barriers between these frequently siloed capabilities, to reduce complexity, streamline operations, and benefit from synergies that otherwise are not achievable.

By providing deep integrations with freedom of choice from extensive list of leading cloud service providers, Veritas enables you to accelerate your own digital transformation with all the benefits of unified enterprise data protection, delivering seamless, automated data lifecycle management and governance – be that protection of your data and applications in your data centers, remote branch offices or in the cloud.

We invite you to explore the new possibilities presented by 360 Data Management™ and Unified Data Protection.