Why You Need to Transform Your Data Protection

Modern businesses are faster, more dynamic, and more data-driven than ever before: A mechanical engineer whisks designs halfway around the world and gets them back the next business day – from his smartphone; the Internet of Things spins out countless bits of information that yield unimagined insights – and winning business strategies.

These exciting times are not without challenges for IT. The new ways of doing business rely on larger quantities of more critical data than ever before, making data loss increasingly unacceptable. And yet security threats are more numerous and more varied, and natural disasters continue to loom menacingly over data centers. Migration from legacy technologies like Windows Server 2003 requires modernized infrastructure. If that weren't enough, the cloud has taken its place as an important piece of the IT puzzle – and yet, effective management of data in the cloud remains uncharted territory for many.

NetApp

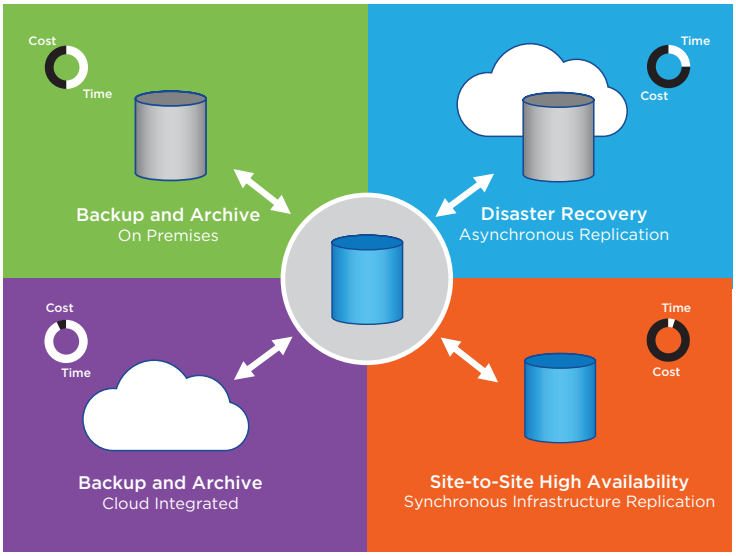
CIO
Strategic Marketing Services

Why Businesses Need a New Approach to Data Protection

When organizations try to enable new business models while maintaining their traditional approaches to data protection, they quickly run into barriers. Previous methods are simply not sustainable due to complexity, cost, and inefficiency. But change often comes too slowly to data protection architectures.

Consider the traditional model: In the primary data center, primary storage is backed up first to disk and then to tape. Tape copies are transported regularly to an offsite storage facility for recovery purposes in case of disaster. At the same time, primary storage may be replicated to secondary storage at a secondary data center. Although it provides high availability, replication can be costly.

NetApp Data Protection Model



While the traditional approach was effective in its time, it has several shortcomings that become even more acute as IT modernizes its infrastructure. Traditional replication creates complexity and management headaches as copies of data are sent from one site to another. Tape backup is unwieldy because it depends on the ability of a vendor to reliably transport tape cartridges to an offsite facility for either storage or disaster recovery. Much can go wrong in this seemingly straightforward process: Tapes can be misplaced, broken, left on a loading dock, or even stolen – never to serve their intended purpose of keeping an organization afloat when a primary data center is hit with a power outage or natural disaster.

Downtime and data loss are costly. A 2013 Aberdeen study found that IT downtime costs businesses an average of more than $163,000 an hour.[1] In addition, the threat of data breaches continues unabated, with consequences that can be devastating to a business's finances and reputation. Cyber attacks cost the average U.S. company $12.7 million in 2014, a 9% increase over the prior year, according to the Ponemon Institute.[2] Faced with burgeoning security threats, encryption of data both in flight and at rest is indispensable. And yet, too often, encryption has not been consistently implemented in the traditional approach to data protection.

The Four-Quadrant Data Protection Model

As the effectiveness of traditional approaches wanes, technology innovations and the cloud are creating new possibilities for data protection. IT execs are catching on: Three of the top ten IT spend categories for 2016-2017 will be in data protection, according to ESG.[3]

But new technologies alone are not enough. New approaches must reflect a thorough rethinking of the relevance of different types of data to the business. Increasingly, IT managers are discovering that the best data protection architectures eliminate the use of tape and all the challenges it entails.

The NetApp® data protection model gives managers a way to look at data protection from a macro level and pick a solution that balances cost, recovery time, and risk. Two quadrants are in the category of backup and archive. The other two are in the category of disaster recovery.

[1] "Downtime and Data Loss: How Much Can You Afford?" August 2013, Aberdeen Group
[2] "2014 Cost of Cyber Crime," Ponemon Institute, 2014
[3] "2015 IT Spending Intentions Survey," ESG, February 2015

SUCCESS STORIES

Here's how two companies transformed their data protection.

Spot Trading, a technology-focused proprietary trading firm headquartered in Chicago, was finding that time-consuming and costly data protection processes were impeding its growth. A full week each month of one person's time was required to back up systems and securely store trading logs, email, and other communications. Data restores took one or two people up to three days. IT needed a better approach – one that would free up its IT team for more strategic endeavors.

Spot Trading chose cloud-integrated backup and archiving – a combination of NetApp AltaVault® cloud-integrated storage and the Amazon Web Services (AWS) Glacier storage service. For a low monthly storage cost per gigabyte, Spot Trading gained compression, deduplication, and data encryption for data both in flight and at rest.

The savings in time and money have been striking. By eliminating the tape library and cancelling the company's tape management service, the firm reduced its annual archival storage utilization and cost by 96%. In so doing, Spot Trading recovered 40 hours per month for the IT team to spend working on new strategies and systems. In addition, Spot Trading data can be restored in minutes at the click of a mouse, instead of two to three days with tape.

By moving storage to the cloud, the company achieved additional savings by avoiding spending $500,000 on a SAN upgrade.

Blach Construction differentiates itself from other construction companies through its commitment to sustainability as well as in its use of technology to help ensure profitability in a very cost-competitive business.

Challenges for Blach's very small IT team include backing up ever-expanding volumes of data, planning for disaster recovery, and making decisions about where to host various services (cloud versus data center versus headquarters) in the firm's increasingly hybrid IT environment. Solutions from NetApp help make all of this possible.

The company chose Amazon S3 as its cloud storage provider and a NetApp AltaVault cloud-integrated storage appliance. The main benefit of replacing SAN-to-SAN backup with AltaVault and Amazon S3 is having nearly 20 hours returned to the business each month. The time saved is being used where the business needs it most—improving the IT infrastructure at job sites—so that people there can use the same advanced collaboration tools that they use in the home office.

AltaVault also gives Blach's IT team greater confidence in its ability to recover data, especially after a disaster. Recently, a data restore from the cloud took around an hour, something that would have taken many hours on the old tape system and would not have been nearly as reliable.

Blach Construction's use of NetApp solutions as both a competitive advantage and as one more way the company stands out.

Here's a look at each:

1 CLOUD-INTEGRATED BACKUP AND ARCHIVE

Data protection is one of the most useful ways to realize the full potential of the hybrid cloud. This solution relies on the public or private cloud for storage that delivers the benefits of low cost and highly elastic capacity. Of the four quadrants, this is the lowest-cost approach and is appropriate for data that does not require instantaneous restore. However, if data is not also cached locally, it can lead to long restore times as data is pulled back from a cloud provider.

2 ON-PREMISES BACKUP AND ARCHIVE

Backup and archive that is done either locally or site-to-site delivers a more rapid restore from a given point in time, at a somewhat higher

cost than the cloud-integrated approach. This approach is applicable for information that is highly sensitive or must be kept locally due to compliance requirements.

3 DISASTER RECOVERY

An asynchronous mirroring approach enables organizations to address site failures and to recover operations at a second site. This approach is appropriate for data that must be recovered quickly, but not instantaneously, and where minimal data loss is acceptable. Asynchronous mirroring is more costly than either of the backup and archive options, but it represents an economical approach to disaster recovery.

4 HIGH AVAILABILITY

Synchronous replication enables failover from one active site to another, resulting in zero data loss and near-instant recovery. It is typically more expensive than equivalent asynchronous solutions due to additional equipment and data networking requirements. This approach is appropriate for data with the highest criticality.

Selecting the Right Solution

Faced with these options, where should you begin? First, step back and consider your data holistically. Different types of data have particular data protection needs and economics. Work with your business continuity counterparts to establish acceptable recovery time objectives (RTOs), recovery point objectives (RPOs), and the cost of downtime for each. A business impact assessment (BIA) is a good place to start. The values you assign will determine the backup and disaster recovery technologies you select.

Your data priorities should be based on a scale ranging from mission-critical, such as transactional databases, down to non mission-critical, such as home directories. Although all data categories may seem important, the most critical data is the data without which your company cannot remain in business.

Because you are looking at your data holistically, you need tools that will enable you to manage it across the full data protection spectrum. Since many organizations are already using products from providers such as CommVault, Veritas, or Veeam, a data protection architecture that interoperates with these technologies will leverage investments you've already made, saving time and expense. The tool you select should enable you to manage all categories of data across the full portfolio of data protection technologies. A comprehensive, easy-to-deploy solution can make a huge difference in the cost-effectiveness of your strategy.

Finally, select and deploy solutions from each of the four quadrants according to your needs.

Conclusion

New business strategies are giving forward-thinking organizations a competitive edge. However, data protection strategies that may have been good enough just a few years ago are no longer sufficient. Data protection technologies are at an inflection point: More efficient and less costly storage, both on-premises and in the cloud, is making tape and all its operational headaches obsolete.

It's time for IT leaders to closely examine their businesses' data-protection requirements. The goal is to find the right balance between data protection capabilities and cost. NetApp's four-quadrant data protection model, which covers the full spectrum from cloud-integrated backup and archive to site-to-site high availability, is the most effective template to address these needs.

The ability to obtain all four types of data protection technologies from a single provider enables your organization to look at data protection holistically, as an entire data fabric. The result: the ability to meet your data protection needs in an efficient and streamlined manner, matching data, cost, and purpose with the right data protection technology. ■

To learn more about solutions to transform your data protection, visit **www.netapp.com/data-protection**.