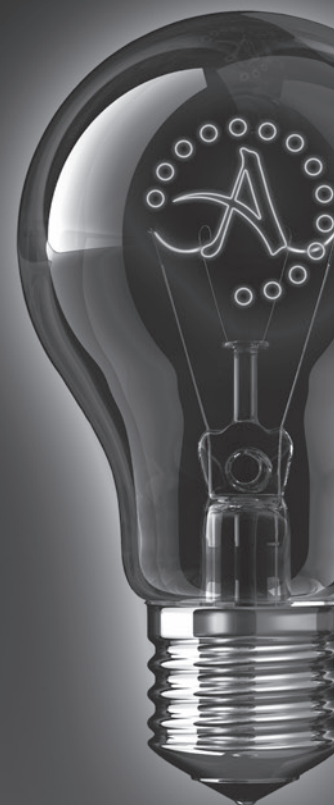


# *Why Cloud and How to Choose a Cloud Vendor*

*Autonomy White Paper*



# *Index*

Why Cloud and How to Choose a Cloud Vendor	1
<i>Cloud-based Data Protection</i>	2
<i>Benefits of Cloud Backup</i>	3
<i>Selecting The Right Cloud Storage Service Provider</i>	4
Conclusion	5
About Autonomy	5

# Why Cloud and How to Choose a Cloud Vendor

The demand for data storage is exploding, which is driving up costs, amplifying the risks of data loss or exposure, and complicating plans for disaster recovery. To cope with this exploding demand, organizations are turning to cloud-based storage for relief. The adoption of cloud solutions is growing, with a nearly 40 percent expansion in the use of third-party cloud storage for offsite copies expected by 2012 (*"Data Protection Trends,"* ESG, April 2010).

At the same time, mid-sized enterprises are migrating away from tape backup. They are trying to extricate themselves from the complex infrastructure and burdensome responsibilities of tape hardware, tape libraries, and complex and error-prone tape-based processes. Organizations are finding cloud-based data protection to be especially attractive, effectively reducing the cost of ownership associated with the entire backup infrastructure of disk, deduplication disk, tape, tape libraries, backup servers, and other components. Cloud-based data protection also lowers the cost of downtime from an emergency such as a natural disaster. For IT departments asked to do more with less, this is a welcome solution.

Furthermore, enterprises must also deal with the unsettling fact that traditional backup methods still cannot guarantee 100-percent-successful data recovery. *What's the point of backing up your data if you can't get it back when you need it?*

Moreover, most organizations now face requirements for compliance and eDiscovery. Therefore, gaining accessibility, visibility, and control over your organization's data across applications, laptops, and desktops is not only important for business continuity, but it's also a legal obligation that most companies today must satisfy.

These organizations are discovering that the sooner cloud-based storage appears in their processes, the greater the benefits they enjoy. They are even finding that they can eliminate their onsite, disk-based backup and archiving in favor of cloud-based data protection.

## Benefits of the Cloud

- Avoid Capital Expenditure and Infrastructure Costs
- Information Management Applications as a Service
- On-Demand, Pay-As-You-Go
- Guaranteed Service with Service Level Agreement
- Improve Disaster Recovery

## Cloud Provider Checklist

- Track Record
- Physical Security
- Data Security
- Geographic Availability
- Data Availability
- Scalability
- Optimization
- Flexibility
- Simplicity
- Minimizes Risk

## Cloud-based Data Protection

For data protection, tape was a first-generation solution — lacking rapid and guaranteed recovery — and disk was a second-generation solution — lacking offsite, scalable, and low-cost storage. However, with the right vendor to satisfy your business requirements, cloud backup is the next-generation solution that can meet your company’s data protection needs. You no longer have to stick to tape or on-premises disk-based backup.

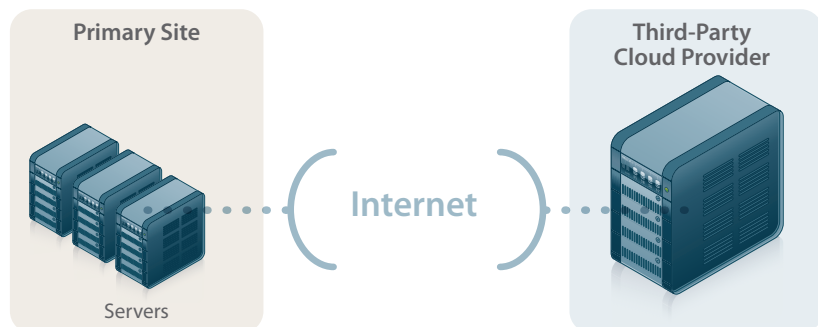
Traditionally, you back up your data to your primary data center. You probably use another data center as a second site for disaster recovery purposes. However, this traditional arrangement poses many challenges. On-premises backup requires large and continuing capital investment costs for equipment and infrastructure. Worse, you and your staff must shoulder the burgeoning responsibility for managing this disk and tape conglomeration. Repurposing or reconfiguring equipment for other uses becomes a complex and cumbersome process that inhibits you from satisfying your mandate to “do more with less.” Furthermore, because mobile laptops, remote offices, and branch offices must use your LANs or WANs for backup, your network capability drops and the protection of these most-vulnerable resources becomes less certain and more risky. As a result, your disaster recovery stance is worse.

However, by skipping your on-premises disk-based data centers and using third-party cloud-based data protection as your second site, you can achieve the same backup and recovery goals, and avoid all these challenges. There are no capital investment costs, because the storage infrastructure is offsite at a secure facility. Professional and experienced staff who are experts at data protection take charge of your data and provide results guaranteed by service level agreements (SLAs). This frees up your resources for more nimble repurposing. In addition, mobile laptops, remote offices, and branch offices can connect directly with cloud-based data protection, relieving the burden on your network infrastructure, and improving the protection of these data assets. The bottom line is a significant improvement in your disaster recovery capabilities, reduced capital expenditure, more time to devote to more strategic programs, and greater freedom to deploy resources.

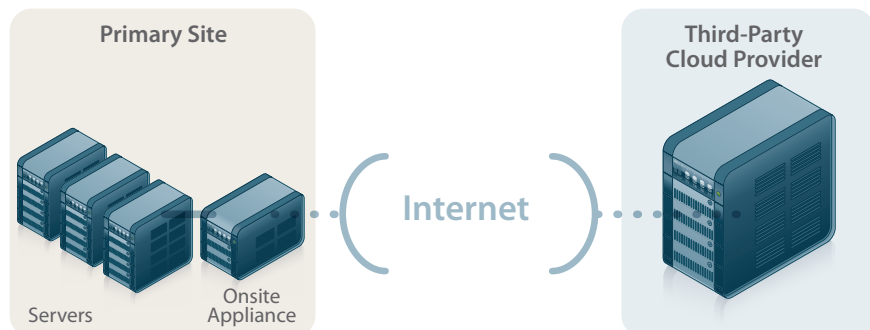
There are two strategies for skipping the disk and archiving directly to cloud-based data protection, called Disk-to-Cloud (D2C) and Disk-to-Disk-to-Cloud (D2D2C).

With the Disk-to-Cloud strategy, you back up your data to a cloud provider directly. With the Disk-to-Disk-to-Cloud strategy, you back up your data to a local appliance first, and make the cloud provider your second site. The difference is that the D2D2C strategy can offer better performance for recovering bulk data from a local appliance, which can be very useful if you have limited bandwidth.

### Disk-to-Cloud (D2C)



### Disk-to-Disk-to-Cloud (D2D2C)



## Benefits of Cloud Backup

If you choose the right cloud-based data-protection provider, then backing up data to the cloud has many benefits.

**1. Avoid Capital Expenditure And Infrastructure Costs:** The pay-as-you-go model for cloud-based data protection helps you reduce or avoid capital expenses. Using the cloud also lets you avoid adding more and more tape, secondary disk, and deduplication infrastructure to your data center.

**2. Information Management Applications As A Service:** By using cloud-based data protection, you shift the burden of the complex backup process, technology, and management to the experts at Autonomy. Your backup and recovery process becomes seamless, reliable, and secure.

Because your data is securely backed up to Autonomy's off-premises data centers, your own servers and infrastructure are available for other purposes. This improves the agility of your enterprise to compete successfully.

With data safely stored in a professionally managed cloud-based data protection service, you also reduce your own burdens and the responsibilities of managing the complex and error-prone data protection process. Your IT staff can then focus on more strategic projects for your company.

Cloud-based data protection can also improve your support for remote offices and branch offices. Instead of burdening your enterprise WAN or LAN, they can interact directly with the cloud.

**3. On-Demand, Pay-As-You-Go:** Because of economies of scale, cloud-based data protection is often more cost-effective than in-house solutions, removing capital expenditures and allowing pay-as-you-go financing. You can avoid the unpredictable—and often hidden—costs of in-house storage by selecting a cloud service provider who offers a predictable rate that makes your budgeting simpler.

We've all experienced delays in version upgrades due to busy schedules. Cloud service providers offer the latest versions and upgrades in storage, security, and data transfer technology, without taxing your own IT resources.

A well-managed cloud service means that the service provider proactively monitors and tests for all potential vulnerabilities and detects all possible threats. If the vendor's reputation depends on their security, their IT can be more secure than your own.

**4. Guaranteed Service With Service Level Agreement:** Instead of assuming the liability of your unpredictable in-house service, you can hold the service provider accountable for service-level deliverables—including recovery time objectives (RTO), recovery point objectives (RPO), and uptime—guaranteed by a written Service Level Agreement (SLA).

**5. Improve Disaster Recovery:** Storing data remotely with a trusted cloud-storage service provider automatically gives you an offsite copy of your data. This immediately helps you to meet your disaster recovery requirements, at a fraction of the cost. According to research by ESG, satisfying disaster recovery requirements is one of the top reasons why companies make cloud-based data protection part of their data protection strategy. In addition, by moving your data offsite, you improve your long-term retention capability, as well as your compliance stance.



## Selecting The Right Cloud Storage Service Provider

You can only achieve the many benefits of cloud-based backup if you select the right cloud service provider. Here are some characteristics of the ideal cloud service provider that you should consider:



**1. Proven Track Record and Extensive Experience With Managing Customer Information:** The cloud service provider must have a proven history of extensive experience managing customer information and protecting that information for the long term. Look for consistent longevity in service and a superb reputation in the marketplace.

The physical data centers of the service provider must represent the highest levels of security against both intrusion and acts of nature. Does the vendor rent or own these data centers? Does the vendor have strict policies in place for anyone who might have access to your data? Look for vendors who make security their highest priority.

Data security is more than encryption. The service provider must demonstrate the strictest processes and technologies to safeguard your data, including written policies for proactive monitoring, data encryption in transit, encryption during storage, encryption key escrow management, controlled access, and verification of data integrity.

**2. Geographic Locations To Support Worldwide And Local Requirements:** The service provider must operate physical data centers in geographically separate areas, to satisfy compliance and access concerns. A worldwide presence helps customers with international offices to achieve efficient recovery, support local needs, and meet local regulatory requirements.

**3. Scalability:** The service provider must be able to accommodate the growing and difficult-to-predict data storage needs of enterprise customers, using built-in technologies for deduplication, storage, and data transfer. In addition, retention choices must be flexible enough to manage capacity, costs, and regulatory requirements.

**4. Flexible Retention And Configuration:** On-Premises, Cloud-Based, And Hybrid: The service provider must be able to support your own needs and approaches to retention and configuration. Choices for backup and archiving should include many options, such as:

- *On-premises (licensed)*
- *Disk-to-Cloud (hosted)*
- *Disk-to-Disk-to-Cloud (hosted plus onsite appliance)*
- *Hybrid (remote managed services)*

**5. Reliable And Simple Data Recovery:** The service provider's solution must be easy for you to set up and use, with automatic set-and-forget operation that requires no training. The service should be fully managed, with proactive notification.

The ability to access and recover data is crucial. Redundant facilities must be in place to guarantee the availability and recoverability of data. Furthermore, recovering data from the cloud must be a simple and reliable process. The vendor must demonstrate the ability to restore data even if your encryption key custodian leaves your company.

The service provider must offer solutions to enable you to efficiently and rapidly restore data — from a single file to an entire site failure — under your constraints of capacity and bandwidth, and meet your RTO/RPO requirements.

The service provider's continuous backup technology and mirrored data centers must minimize your risk of data loss, as well as your cost of downtime in an emergency.

# Conclusion

Enterprises that are ready to skip the disk and move to the cloud have the opportunity to obtain great benefits from a simpler, less expensive, and more powerful process. By selecting the right service provider, your enterprise can leverage the capabilities of the cloud for long-term and significant advantages.


## About Autonomy

Autonomy Corporation plc (LSE: AU. or AU.L), a global leader in infrastructure software for the enterprise, spearheads the Meaning Based Computing movement. IDC recently recognized Autonomy as having the largest market share and fastest growth in the worldwide search and discovery market. Autonomy's technology allows computers to harness the full richness of human information, forming a conceptual and contextual understanding of any piece of electronic data, including unstructured information, such as text, email, web pages, voice, or video. Autonomy's software powers the full spectrum of mission-critical enterprise applications including pan-enterprise search, customer interaction solutions, information governance, end-to-end eDiscovery, records management, archiving, business process management, web content management, web optimization, rich media management and video and audio analysis.

Autonomy's customer base is comprised of more than 20,000 global companies, law firms and federal agencies including: AOL, BAE Systems, BBC, Bloomberg, Boeing, Citigroup, Coca Cola, Deutsche Bank, DLA Piper, Ericsson, FedEx, Ford, GlaxoSmithKline, Lloyds Banking Group, NASA, Nestlé, the New York Stock Exchange, Reuters, Shell, Tesco, T-Mobile, the U.S. Department of Energy, the U.S. Department of Homeland Security and the U.S. Securities and Exchange Commission. More than 400 companies OEM Autonomy technology, including Symantec, Citrix, HP, Novell, Oracle, Sybase and TIBCO. The company has offices worldwide.

Please visit [www.autonomy.com](http://www.autonomy.com) to find out more.

Autonomy and the Autonomy logo are registered trademarks or trademarks of Autonomy Corporation plc. All other trademarks are the property of their respective owners.



*The information contained in this document represents the current opinion as of the date of publication of Autonomy Systems Ltd. regarding the issues discussed. Autonomy's opinion is based upon our review of competitor product information publicly available as of the date of this document.*

*Because Autonomy must respond to changing market conditions, it should not be interpreted to be commitment on the part of Autonomy, and Autonomy cannot attest to the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. Autonomy is not making warranties, express or implied, in this document. Autonomy and the Autonomy logo are registered trademarks or trademarks of Autonomy Corporation plc. All other trademarks are the property of their respective owners..*

*Autonomy Inc. and Autonomy Systems Limited are  
both subsidiaries of Autonomy Corporation plc.*

20110816\_RL\_WP\_ROI\_for\_Cloud\_Data\_Protection

