

Field Audit Report

Asigra

Hybrid Cloud Backup and Recovery Solutions

By Brian Garrett with Tony Palmer

May, 2009

Contents

Introduction	3
Background	3
Customer #1	5
Customer #2	7
Customer #3	9
ESG’s View.....	11

ESG Field Audits

The goal of the ESG Field Audit is to educate IT professionals about emerging technologies and products in the storage, data management and information security industries. ESG Field Audits are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies as they are being applied in end-user environments. ESG’s expert third-party perspective is based on interviews with customers who use these products in production environments. This ESG Field Audit was sponsored by Asigra.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. Copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482.0188.

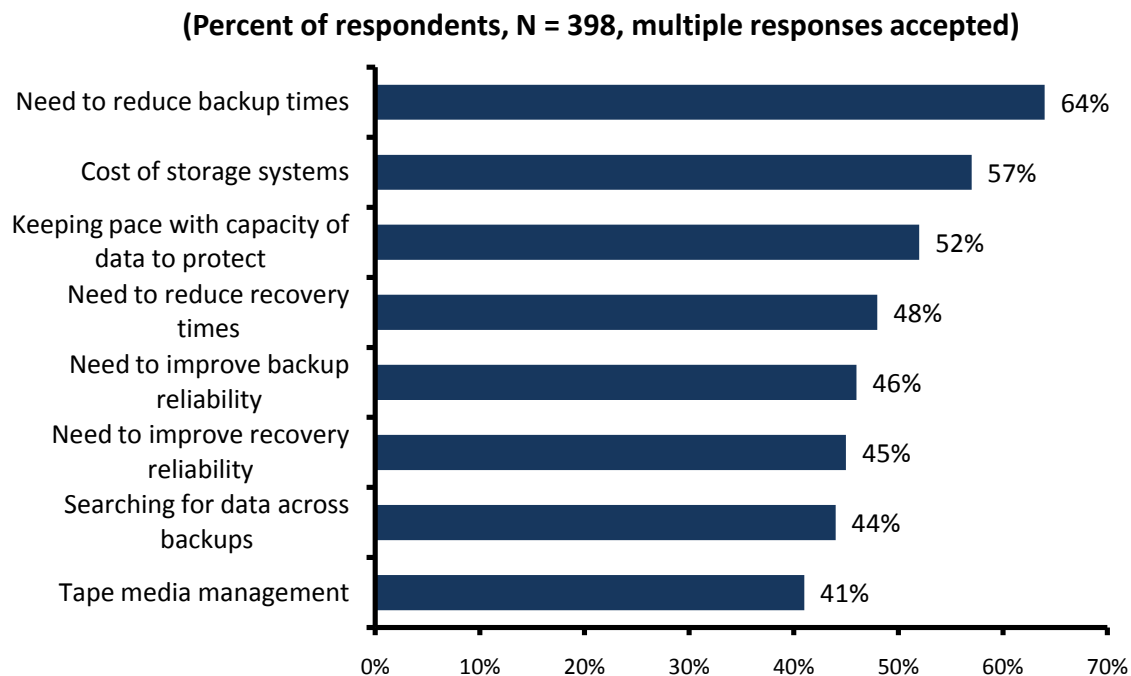
Introduction

ESG recently completed interviews with customers using Asigra Hybrid Cloud solutions for backup, recovery disaster recovery, and compliance. This ESG Field Audit documents the successes of these customers as Asigra Hybrid Cloud solutions are used to protect information stored on servers, virtual machines, desktops, and laptops.

Background

Organizations of all sizes are struggling with the risks and costs associated with protecting information. ESG Research has found common challenges between businesses large and small with current backup methodologies and technologies.¹ As shown in Figure 1, the time and effort expended performing backups and recoveries; the reliability of backups and restores; and the costs of acquiring, managing, and upgrading tape and storage systems were all identified as top challenges. Enterprise and small business respondents identified tape media management for onsite and offsite requirements as a challenge.

Figure 1. Data Protection Process and Technology Challenges



Source: Enterprise Strategy Group, 2009.

A growing number of IT managers are using cloud computing principles to address their data protection challenges. The key advantage of a cloud computing approach to backup and recovery is the ability to use wires full of data—instead of trucks full of tape—to send backups to a remote site for compliance and disaster recovery. Cloud backup services can be outsourced as a service running over the Internet (public cloud) or implemented within an organization’s existing corporate network (private cloud). A hybrid cloud approach offers the best of both worlds: some of the tasks can be outsourced to run over a public cloud and others deployed within a corporate network on a private cloud. It can be implemented exclusively at a cloud-connected remote location (off-premise) or it can be deployed with the addition of local servers providing a cached copy of the latest backup data for quick and reliable ad-hoc recoveries (on-premise *and* off-premise).

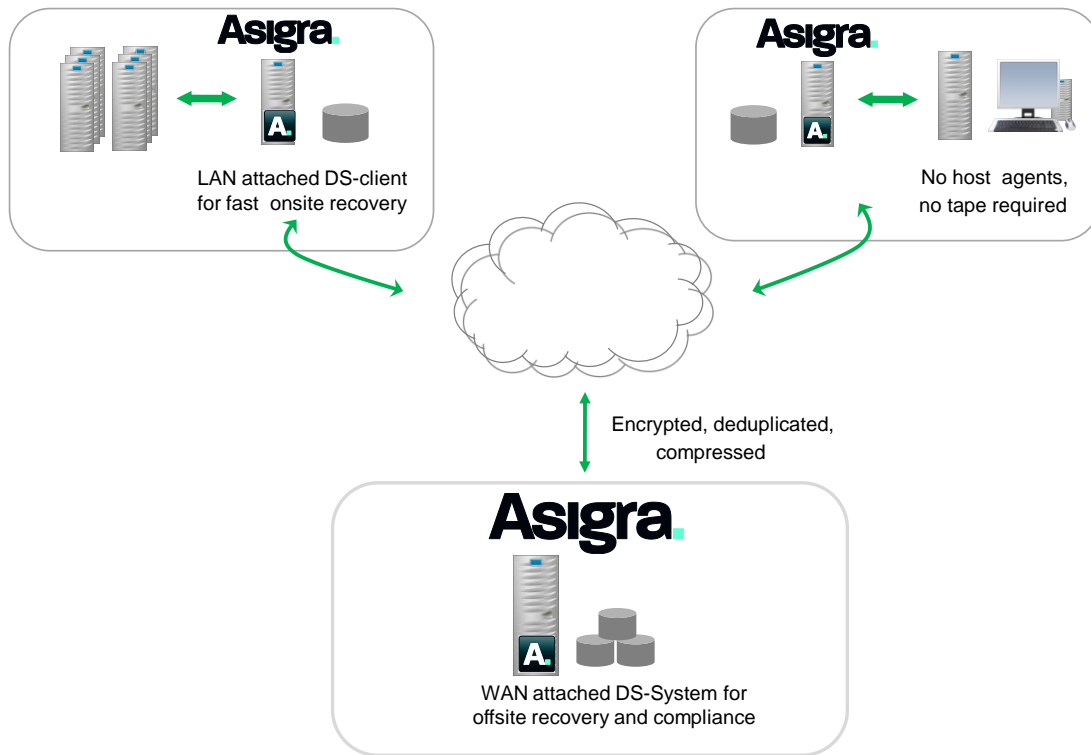
Asigra uses a hybrid cloud approach to help businesses recover lost information residing on servers, virtual machines, desktops, and laptops. Asigra began providing cloud backup and recovery services long before the term “cloud computing” became popular. Often sold by well-known telecommunication companies and service

¹ Source: ESG Research: *ESG Data Protection Survey*, January 2008.

providers, Asigra solutions have been deployed by thousands of organizations with tens of thousands of remote sites.

An overview of a typical Asigra Hybrid Cloud backup and recovery solution is shown in Figure 2. Data located in servers and workstation within two corporate offices is sent through a cloud to a WAN-attached server for offsite recovery and compliance. An optional LAN-attached client running Asigra software is used as a staging area for backup data, enabling quick and reliable onsite recovery. Data is deduplicated, compressed, and encrypted before it is sent through the cloud to a remote site. Asigra uses industry standard data access methods, which eliminates the need for host agents. Tape is not required.

Figure 2. Hybrid Cloud Backup and Recovery Services



Source: Enterprise Strategy Group, 2009.

ESG Lab tested an Asigra solution in early 2005 and validated that a hybrid cloud approach can be used to protect an organization's data in multiple locations while minimizing storage and WAN bandwidth requirements. We were impressed by both Asigra's overall approach and its ability to efficiently protect remote and branch offices. The combination of data de-duplication, continuous data protection, and data compression changes the economics of backup and enables customers to reduce the amount of WAN bandwidth utilized, while reducing the amount of storage capacity required to store backup data. This reduces both storage acquisition and recurring service charges over time. The Asigra solution also eliminates the need for agents, offers a high level of security, has excellent reporting tools, and is extremely reliable and scalable.

As a complement to our hands-on testing in a laboratory setting, ESG recently spoke with three IT managers using Asigra Hybrid Cloud solutions in production environments. The organizations varied in size and complexity—from a web design and hosting company serving thousands of clients on shared infrastructure to a major international trading and distribution firm with more than 50 offices distributed in as many countries.

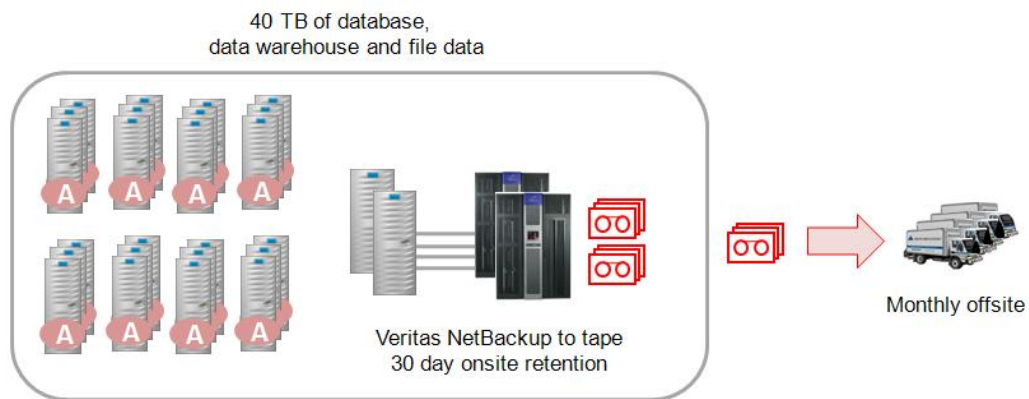
Customer #1

ESG spoke with the IT Infrastructure Manager of a regional manufacturing division of a global corporation that sells millions of its products to consumers worldwide every year. The infrastructure group is responsible for five services: security, databases, data warehouse, UNIX storage, and backup.

The Environment

Before we implemented Asigra, we had about 300 physical servers housing a total of 40 TB of production data in one location. Our most critical applications are supporting the production line. They're mostly home grown applications running on SAN-attached servers. We were using two Veritas NetBackup media servers and StorageTek SDLT tape silos. We ran weekly full and daily incremental backups. Full backups were sent offsite weekly. More than 700 tapes were sent offsite every month.

Figure 3. A Manufacturing Production Environment Before Asigra



The Situation

We were exceeding our backup windows on file and SAP data. We had 2 TB of file shares with no archiving. Users were forced to purge files periodically to keep the data set manageable. The decision had been made to expand operations into a second data center and we knew the existing backup infrastructure was not capable of handling the additional load. We evaluated the relative merits of adding to the existing environment vs. fundamentally changing the way we do backups.

The Integration

Asigra was easy to deploy. Since it's agentless, we were able to roll it out as fast as we could get production systems off the previous backup infrastructure. When we added our second location, we set up a private cloud with an Asigra server and client at each site. We're using SAN disk capacity for local cache. Each data center protects the other for disaster recovery.

The Results

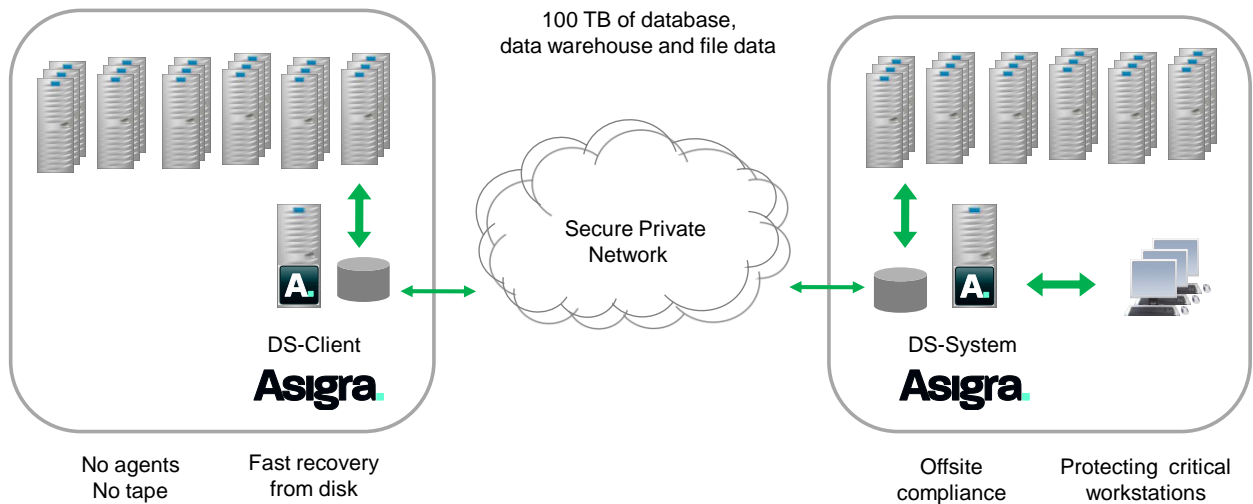
We've been very happy with the Asigra solution in general and the simplicity of operations in particular. It's an agentless system with clean, easy to use interfaces. Tape was always an operational challenge. When managing media, backup software, and clients, we constantly had to deal with compatibility. New software releases caused integration issues between the media servers and the agents. Reporting with Asigra is much easier as well. We did not have to purchase any additional software as we would have with NetBackup. We have no formal service level agreements, but backups and restores are faster and more reliable. Our goal was to maintain our FTE (full time employee) count and we've been able to do that. We're protecting 2.5 times the data in two data centers with the same FTE count as we had 2 years ago in just one location. Asigra is an excellent solution for backup and recovery. I

don't know why more people aren't doing it this way. It looks like the industry is moving in this direction, but many users seem to let budget constraints be an issue before examining the true cost savings. If people experienced it, they'd be able to properly assess it.

The Configuration

This customer expanded operations to a second location and installed an Asigra DS-Server and client on each SAN with local caching to provide better performance for local restores. They maintained about the same number of physical servers, but are now protecting about 100 TB across their two data centers. An Asigra BLM Archiver server is installed in one data center, providing a repository for archived file and e-mail data. Additionally, this customer was able to provide protection for custom workstations that provide mission critical production support

Figure 4. A Manufacturing Production Environment After Asigra



Why This Matters

Within organizations of all sizes, traditional backup environments are being stretched beyond their abilities to deliver adequate protection services. IT managers are increasingly being asked to back up and recover more data with stagnant, or shrinking, budgets and staffing.

This Asigra customer is constantly being asked to do more with less. They needed to perform more backups, provide better service levels, and offer a more integrated solution including archiving—all at lower cost and using fewer resources. Asigra helped them achieve that. In addition, mission critical workstations on the production line were able to be protected; this just wasn't possible in their traditional backup environment. From both a time and a technology standpoint, Asigra helped make it possible.

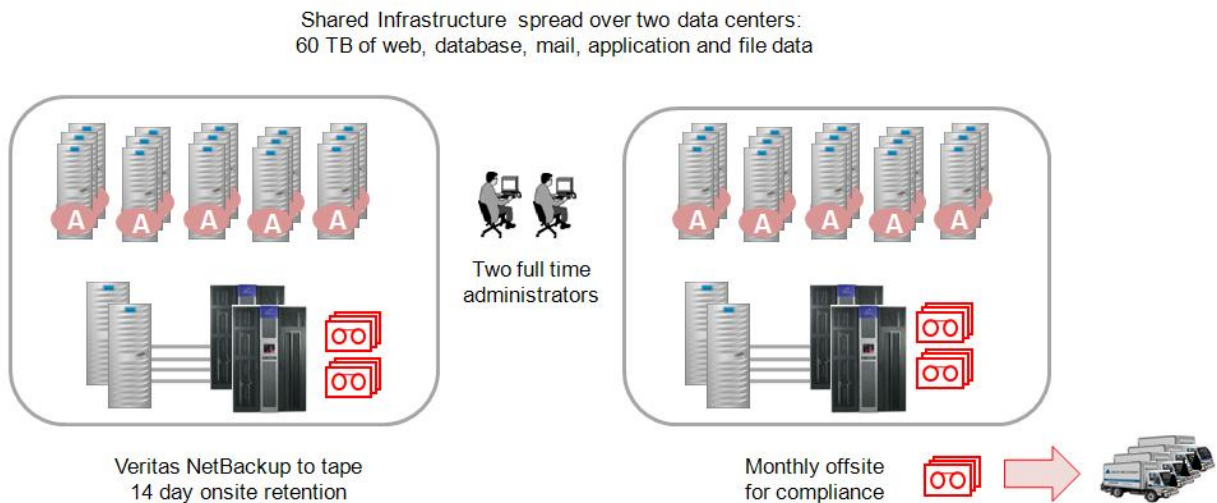
Customer #2

The next IT manager ESG spoke with is the Vice President responsible for IT infrastructure management for a web design, marketing, and hosting company that focuses on small businesses. ESG asked a series of questions to learn how Asigra has changed the way this service provider protects its customers' data. The IT manager began with a description of his IT environment:

The Environment

We had two Data Centers with about 1,500 servers, hosting multiple customers per server. We used Veritas NetBackup to back up all of our customers' data to tape. We were running four NetBackup media servers and had four tape silos. We were backing up about 60 TB of customer data, using weekly full and daily incremental backups and sending full backups offsite monthly. We had two full time administrators dedicated to managing backup and restore.

Figure 5. Hosting Environment Before Asigra



The Situation

We were having numerous problems; the most painful was trying to restore clients' data back to a specific point in time. With thousands of customers on 1,500 servers, there were always multiple restore requests in the queue and sometimes, it would be days before we were able to begin a restore. Then it could take many hours to restore as we were dealing with full and incremental backups to get to the desired point in time. Another major issue was managing the backup agents on the 1,500 shared servers. Any time we updated media server backup software or agents, we had to audit the environment to make sure that the existing agents were compatible.

The Integration

We evaluated a local backup to disk solution before checking out Asigra. The agentless architecture made it a relatively easy deployment. We ran a short evaluation and Asigra has been in production for about a year.

The Results

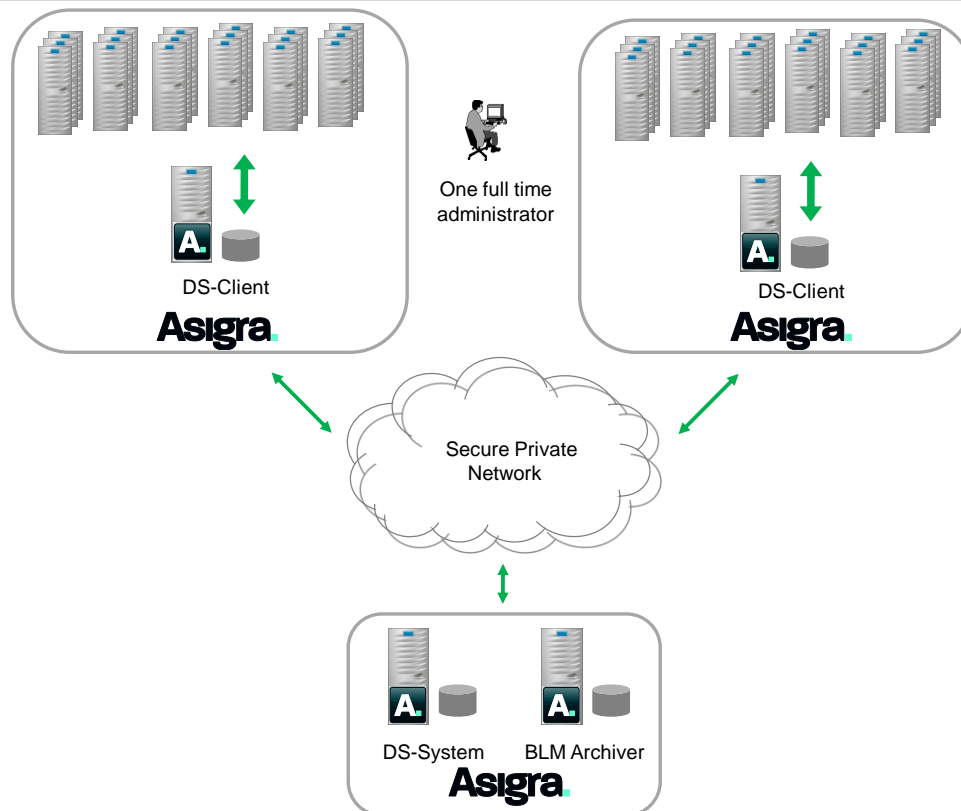
We have improved recovery times and tightened retention times for our production customers. With Veritas, we were storing two weeks of data: two weekly full and twelve daily incremental backups. With Asigra, we store based on file versioning. We are currently storing three generations of files, which gives us much more efficient storage utilization and has enabled us to eliminate time-specific retention periods. We reduced the number of full time

employees dedicated to backup and restore from two to one. We use the BLM (Backup Lifecycle Management) Archiver product in our corporate office to protect both data centers.

The Configuration

This customer installed an Asigra server and client on each SAN with local caching to provide better performance for local restores. They consolidated servers, but are still protecting about 60 TB across two locations. An Asigra BLM Archiver server is installed in their corporate offices providing an offsite target for disaster recovery.

Figure 6. Protecting Thousands of Customers' Data with Asigra



Why This Matters

ESG research repeatedly finds ease of administration and management to be among the most important factors when choosing a backup solution. This is especially important for enterprises with large, complex environments where client backup policies can span thousands of users.

This customer found that Asigra is extremely easy to administer and manage as a private hybrid cloud. By eliminating incremental backups and tape media management completely, administrators were able to concentrate on the data protection needs of their customers. They efficiently deployed and customized the service for their two data centers, implemented DR archiving in a third location while managing bandwidth and storage utilization from a single point of management. Backups and restores complete faster and they've freed up an administrator thanks to server consolidation and simplification of the backup environment.

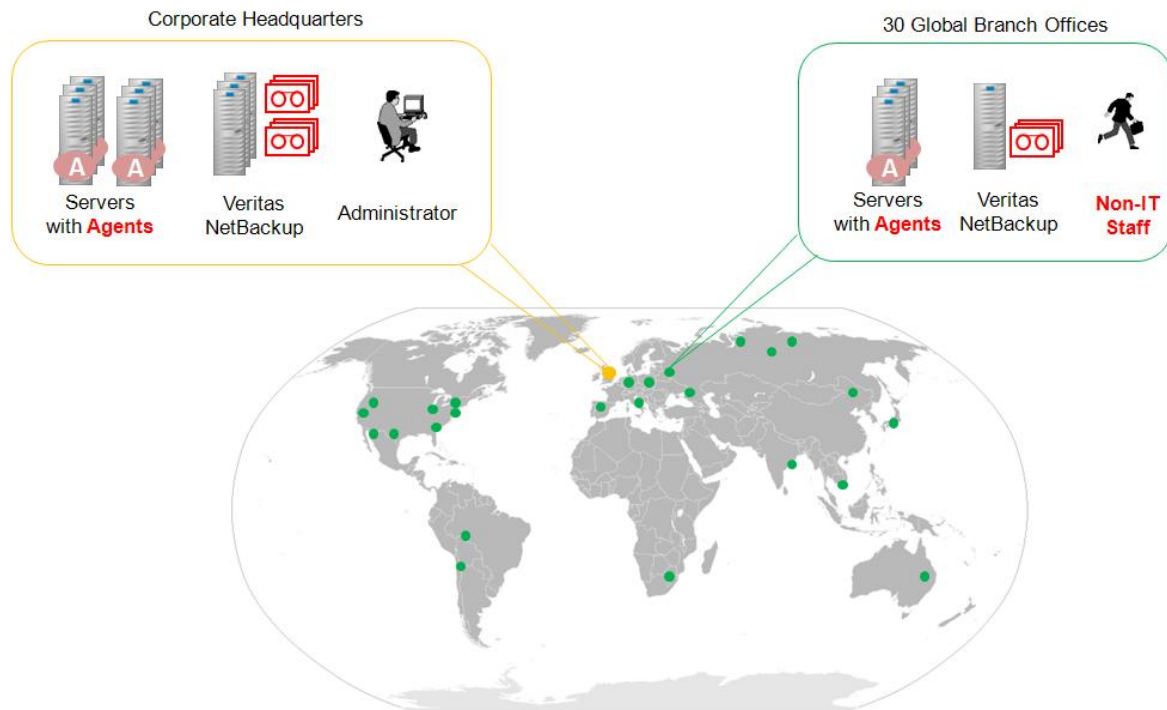
Customer #3

ESG spoke with the IT Technical Manager of an international corporation with more than 50 offices in as many countries. This company trades and distributes raw materials worldwide, providing logistics, financing, and marketing services to their customers. The IT Director had this to say about her environment and the benefits she’s realized with Asigra:

The Environment

I manage servers, the helpdesk, and the IT infrastructure for the entire company. We have about 1,000 users in 58 offices located around the world. We have servers in 30 of our offices.

Figure 7. Distributed Backup Environment Before Asigra



The Situation

Very few offices had IT staff and most had non-technical personnel changing tapes. Managing backups for the 30 remote servers was a huge challenge. It took forever to rebuild a backup from tape. If we didn’t actually have the correct tape, hours were lost and we had to scramble to find the right tape. We ran daily full backups because an incremental policy was too complex to manage in our distributed environment. Restores failed frequently. In one example, e-mail backups in a remote office failed to complete for eight weeks with no indication; then a server failed. Two months were required to recover. Much of the data had to be recovered from users; .PST files. Not an experience I would like to repeat.

The Integration

Asigra was very easy to deploy. We have just the one client at each remote location and no agents to worry about. We’re protecting about 35 servers in 30 locations—all managed by one IT administrator, part-time. Retention policies and offsite retention policies are now part of the backup environment, which we were unable to do before. We retain 28 generations of file backups and 15 generations of SQL.

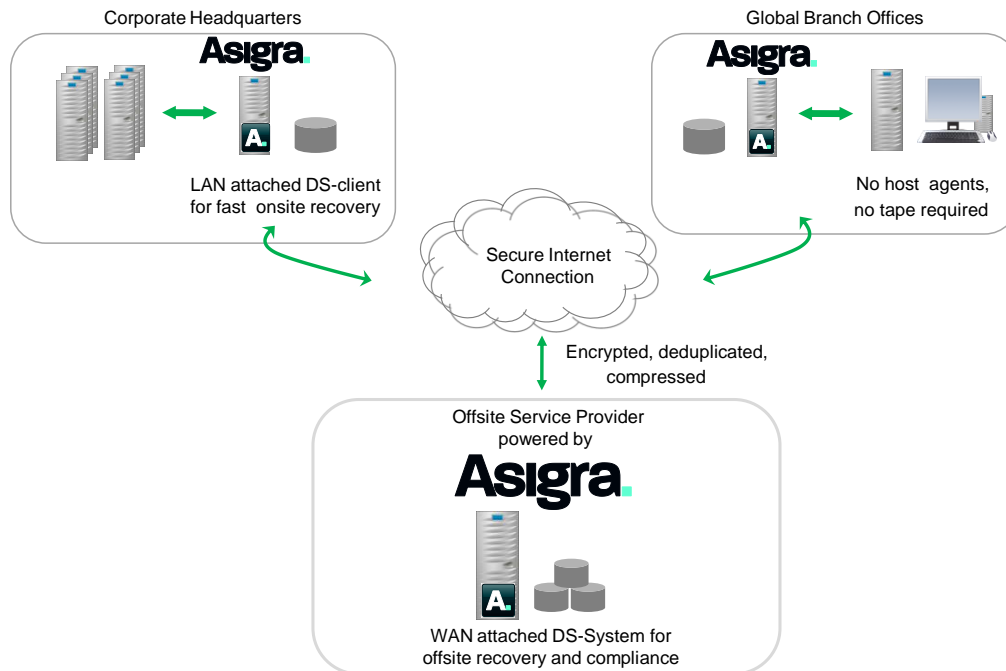
The Results

Our ability to backup and restore data have improved dramatically. We had no IT personnel dedicated to data protection. Backups and restores were being performed by non-IT staff at remote sites. I would definitely recommend Asigra. The Asigra-powered backup solution is very efficient and cost-effective considering the speed of backup and restore and the peace of mind. It's so much easier to manage, especially in a decentralized environment spread around the globe like ours. Everything is managed and monitored from a central point by one person.

The Configuration

Remote offices are protected by a service provider through a public cloud. The service provider installed a server running Asigra software at the corporate headquarters to backup database and file servers. Local cache is used to speed up backups and restores. All remote offices are backed up to the service provider. In a parallel move, e-mail was outsourced to a different service provider that included backup as part of their service. Asigra archive capacity is used to store Microsoft Exchange .PST files from the previous mail system.

Figure 8. Distributed Public Cloud Backup with Asigra



Why This Matters

ESG research indicates that IT managers face a number of significant challenges when trying to protect data at remote locations. Lack of qualified IT personnel at remote locations and concerns about the security of remote backup data were two of the top reported issues. Organizations that have tried to run backups over the WAN using traditional backup software and infrastructure report that backups and restores take too long and the cost of WAN bandwidth is too high.²

This happy customer confirmed that Asigra's Hybrid Cloud Backup architecture addresses all of these challenges. Remote locations are backed up securely and automatically by a service provider. An internal 'virtual cloud' runs at the corporation's headquarters using local cache to optimize restores of critical data. A single administrator manages backup and restore for the entire organization from one location.

² Source: ESG Research Report, *Branch Office Optimization*, January 2007.

ESG's View

Asigra was founded back in 1986 before cloud computing was envisioned. Although the technology has changed dramatically since then, the purpose and architecture have remained surprisingly the same over the years: the idea is to drop a DS-Client (data collector) into a data center or remote office. That single client collects critical data from servers and PC's, massages and compresses the data, and then sends it over an encrypted communications line to a centralized data repository where it is stored safely on disk.

Although backing up to disk is all the rage these days, it was not an obvious solution back when Asigra was founded due to the high cost of disk compared to tape. Similarly, backup as a managed service delivered over a public or private cloud has only recently become economically viable due to the availability of relatively low cost WAN bandwidth. The Asigra solution was built around data reduction and WAN optimization technologies to reduce bandwidth requirements and costs further.

Here in 2009, we spoke with customers using Asigra Hybrid Cloud solutions in a production environment. We also spoke with a customer that has purchased online backup from an online service provider powered by Asigra. That customer's data travels over a public cloud. Others deploy and manage Asigra leveraging a private cloud within their existing corporate network. Together, the customers interviewed by ESG have confirmed the flexibility and value of Asigra's Hybrid Cloud approach to backup and recovery.

Besides the interviews documented in this report, ESG has spoken with a number of IT managers that are redesigning their backup and recovery strategy to take advantage of a Hybrid Cloud approach. Some are being driven by new compliance initiatives. Others are looking for a better way to back up virtual servers. Many are struggling to protect remote and branch offices. Most, if not all, are struggling with relentless data growth and shrinking backup windows. Regardless of the motivation, if your organization is looking for a better approach to backup and recovery, ESG recommends that you follow the lead of the customers interviewed in this report and consider a Hybrid Cloud solution from Asigra.



Enterprise Strategy Group | **Getting to the bigger truth.**