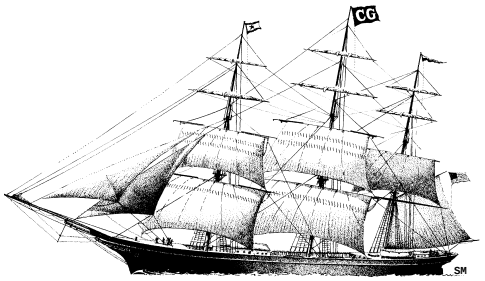
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2006084 September 29, 2006

Asigra Delivers Agentless CDP *for Free*

Analyst: Dianne McAdam

Management Summary

I have lost count of the many offers that I have gotten to receive something for nothing. For example, you can be recipient of this wonderful free necklace (however, please send us a hundred dollars in shipping charges!) Or, how about the email that starts…"I am an unfortunate Nigeria citizen that has millions of dollars stored in a vault that I will gladly share with you…if you send me enough money to get out of here!". My mother always said that if the offer seemed too good to be true…then it probably was. But Asigra has improved on their products and is offering enhancements to their products for free. It is not too good to be true …it is true and it makes good business sense!

Asigra is a small but rapidly growing company in Toronto, Canada, that has concentrated on delivering online backup and recovery products for 20 years. Its backup and recovery product, called *Televaulting*, has been installed by major storage service providers (SSPs), under the brand name of the SSPs, at thousands of customer sites. Recently the company is selling the product direct to enterprises, in particular those with multiple remote locations.

With this latest announcement, Asigra is now providing those service providers and enterprises that have already installed Televaulting and new customers, the option of not only backing up their data but also capturing all changes to their data through Continuous Data Protection (CDP). This new enhancement is available at no extra cost. Asigra is not the first to market with CDP technology, but they are the first to offer this at no additional charge. This gives enterprises more choices when protecting data without costing them extra in licensing fees.

About Televaulting

Asigra's Televaulting software consists of two components. A client resides in the remote site, called the *DS-Client*, and software that resides in a main data center is called the *DS-System*. Asigra's architecture differs from other backup software – no agents are required on the servers and workstations in either location. That makes life simpler for the storage administrator since agents do not have to be installed locally or pushed out to the various locations The DS-Client runs on *Windows*, *VMware*, *Mac OS X* and *Linux*, and can protect data in *Unix*, *Windows*, *Novell*, *Macintosh*, *VMware* and *AS/400* environments, as well as leading databases and email systems, such as *Microsoft Exchange*, *Lotus Domino*, *Microsoft SQL*, *Oracle*, and *DB2*. The DS-System runs on Windows and Linux.

How Televaulting Works

When Televaulting is first installed, all the data at the remote location is backed up, compressed, and encrypted before it is sent to the main location where the DS-System software is installed. During subsequent backups, only the data that has changed since the previous backup is sent to the main location. Sending only changed or new data saves time and money. Backups complete quickly and require less bandwidth to transmit the data and less disk storage to store the backups.

IN THIS ISSUE

Backups are stored in the main location but the most current versions (latest generations) of the backups can also be stored locally at the remote location. Data can be restored from either location, which provides two levels of protection. Data is encrypted at both locations and in flight using up to AES 256 algorithms providing security from unauthorized access. Data deduplication techniques are also imbedded within the Televaulting software to save storage. A *checksum* is generated for each file. This checksum is compared to previously generated checksums. If a match occurs, then Televaulting knows that this file has been previously backed up and will not retransmit the duplicate data. Asigra takes data reduction to an even more granular level. It also divides files into 4K segments and generates a checksum for each segment. Block-level checksum comparisons allow Televaulting to transmit only changed blocks within files – not the entire file. The combination of data deduplication and block-level comparisons can dramatically reduce the amount of data that must be transmitted to the main location.

Asigra not only backs up data but archives it as well. The architects at Asigra recognize that backups and archives are an integral part of Information Lifecycle Management (ILM). Televaulting supports multiple tiers of storage and moves backups among the tiers as needed to meet performance and cost requirements. Inactive data or data that must be retained for a long period of time due to regulations or internal policies can be moved to an archive or vault. Here the data is stored with the version of the software that backed up the data. This ensures that the data can be restored many years later.

How CDP Works

Several vendors offer CDP solutions today. Asigra is not the first to offer CDP, but they are the first to offer agentless CDP. CDP technology comes in two basic flavors – *block-based CDP* and *file-based CDP*. Block-based CDP operates at the logical volume level and records every write, while file-based CDP operates at the file system's level and records any changes to the file system. Some block-based CDP solutions protect data without any understanding of the application. For example, a database transaction may consist of several blocks of data. Block-based CDP records changes to every block. Restoring a database protected by block-based CDP may result in a copy of a database with incomplete transactions. This means that the database must back out these incomplete transactions during its restart process. This adds time to the recovery process.

Asigra has implemented file-based CDP. Files can be restored to the previous changed state. For example, DS-MLR provides CDP protection for email messages. Changes to the messages are recorded after the entire message has been written. Any email message can be restored using Asigra's solution.

Some vendors offer standalone CDP solutions that reside within a SAN and record every write to a protected volume. These solutions require that agents be installed on the servers connected to the CDP appliance. Other vendors offer solutions to protect laptops and remote workstations – again, they require agents be installed on the laptops and workstations.

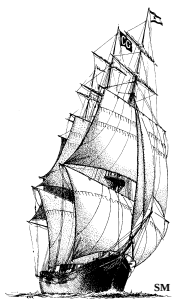
Unlike standalone solutions, Asigra's CDP is integrated within the backup software. Files can be backed up on a regular schedule or protected through CDP. Since CDP continuously captures any updates, the application does not have to be interrupted to perform a backup.

CDP-protected files can be restored from any point in time. That gives enterprises flexibility. More critical files that are updated constantly can be protected with CDP, while less critical files or files that are not updated very often can continue to be backed up as they have in the past.

Conclusion

Asigra is not the first vendor to deliver CDP. But they are the first vendor to deliver agentless CDP. For enterprises with many remote offices, and an even greater number of servers and workstations to protect, having an agentless solution can save time and money and simplify management.

CDP provides a new tier of data protection but is not replacement for existing backup or disaster recovery processes. That is what makes Asigra's solution very appealing. Asigra has added CDP technology to their existing backup, and remote office support. Enterprises can find backup, CDP and support for remote offices all in one solution. Since there are no agents, there are no additional charges for agents. With Asigra, you only pay for the amount of compressed data that is protected. It is a complete solution with a very simple pricing structure, which makes good sense for Asigra and it makes even better sense for enterprises.



About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Dianne McAdam **is Director of Enterprise Information Assurance for the Clipper Group**. She brings over three decades of experience as a data center director, educator, technical programmer, systems engineer, and manager for industry-leading vendors. Dianne has held the position of senior analyst at Data Mobility Group and at Illuminata. Before that, she was a technical presentation specialist at EMC's Executive Briefing Center. At Hitachi Data Systems, she served as performance and capacity planning systems engineer and as a systems engineering manager. She also worked at StorageTek as a virtual tape and disk specialist; at Sun Microsystems, as an enterprise storage specialist; and at several large corporations as technical services directors. Dianne earned a Bachelor's and Master's degree in mathematics from Hofstra University in New York.

- ***Reach Dianne McAdam via e-mail at dianne.mcadam@clipper.com or at 781-235-0085 Ext. 212. (Please dial "212" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group *Captain's Log***, **The Clipper Group Voyager**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, "*Navigating Information Technology Horizons*", and "*teraproductivity*" are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.