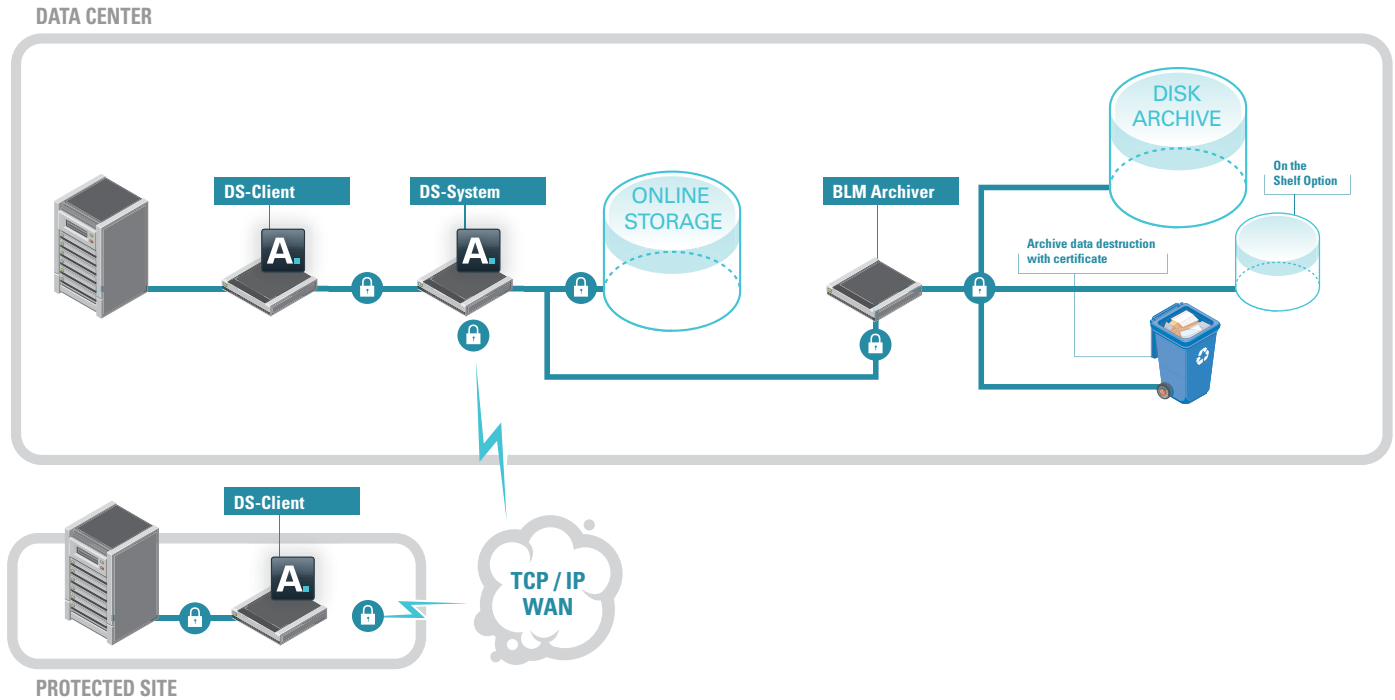


Asigra v9 Encryption, Security, Compliance Advantage



Asigra Encryption Advantage.

Asigra encrypts the data in flight and at rest from cradle to grave.

- FIPS 140 Certified.
- From DS-Client to DS-System to disk to archive and to “On-the-Shelf” archive.
- At rest in the DS-System and in the archive.
- Data destroyed based on policy with certificate of destruction.

Asigra is one of the pioneers in encrypting backup data stored to disk. Its pioneering role was driven in large part by Managed Service Providers (MSPs), who started deploying Asigra as their Information Recovery platform. This made encryption a requirement as far back as 1995, so that MSPs could replicate and store backup data at their data centers.

Since then, Asigra has improved the types of encryption it uses for backup data. Customers can choose from encryption options that range from DES 56-bit with an 8-character key, to AES 256-bit with a 32-character key. Equally important, Asigra maintains

backward compatibility of its software, so that even now, using the current release of Asigra, users can still access and retrieve data encrypted with DES 56-bit encryption years ago.

Furthermore, Asigra v9 is the only data protection software that is certified and compliant with the Federal Information Processing Standards (FIPS) 140 standard. This gives government departments or regulated industries such as financial or healthcare a stamp of approval that they can use Asigra v9 to collect, store and transfer their backup data.

Encryption Key Safeguarding.

Asigra v9 includes an important option that securely and safely manages the encryption keys. Using this feature, customers can securely send and store an encryption key for safe storage in the Data Center vault without risk of compromising the encryption key. This gives them the option to recover their data in the event of a disaster without first needing to locate and produce their encryption key.

In a distributed environment, assume that each site has a site administrator responsible for backup and recovery administration, and assume there is a separate IT contact responsible for the centralized Data Center where the DS-System resides. (A parallel scenario is when the customer install base of a Managed Service Provider has unique DS-Clients installed at their end and the data is transferred over the WAN to the centralized DS-System residing in a MSP's vault).

Asigra customers can take advantage of this feature by configuring the DS-Client at each protected site to forward an encrypted version of the DS-Client encryption keys to the central DS-System for storage in the DS-System database. Because these are stored in this encrypted format, unauthorized personnel are not able to read the encryption key stored in the DS-System. Rather, the DS-System administrator can create a Customer Registration Information (.CRI) file that will be embedded with the information sent back to the IT contact responsible for a particular site.

To ensure administrators at each site are aware that they are agreeing or not agreeing to store their encryption keys with their centralized DS-System, the DS-System administrator can implement Encryption Key Safeguarding in one of three ways:

- **Not support Encryption Key Safeguard at all.** The central administrator may simply elect not to support this option, either because they do not want the liability associated with having the ability to recover the data for individual sites that are manned by their own IT staff, or because they view the risk as too great. In these circumstances, the only encryption option the site administrators have is to assume the encryption key management themselves.
- **Give site administrators a choice.** Some site administrators may not feel comfortable giving the centralized administrator the ability to recover their data, in which case they can continue to use the static encryption key issued to them. Other customers may want this flexibility, so within the DS-Client they select the option that stores the encrypted key on the DS-Server at the centralized location.
- **Force all customers to use Encryption Key Safeguard.** If the DS-System administrator chooses this option, all of the site administrators must escrow their encryption key with them.

Asigra Security Advantage.

Asigra assures secure backup and recovery:

- Zero breaches or compromised systems in over 20 years of operation.
- No open firewall ports.
- Cannot be hacked.
- Data stored in compressed and encrypted format.
- Digital signature for every file and block of data.

- Data on disk in self-describing format.
- Background Autonomic Healing and System Admin (logical check).
- Validation Process (digital signature check).

Password Management and Password Rotation.

Organizations that are extremely security conscious may want to also take advantage of a new feature that gives them the option to automatically generate passwords and change them at random for specific backup user accounts, so that no one can access the account or the data.

Asigra Compliance Advantage.

Asigra v9 can help your business with a variety of compliance issues:

- Disk-based, automated solution that runs quietly in the background with no manual intervention – tape backups require manual intervention and thus are not compliant with regulations like HIPAA and Gram-Leach-Bliley.
- Aggregates all backup data and allows for immediate recovery – traditional backup solutions are not centralized and lead to difficulties in obtaining and providing records to auditors in a timely manner.
- Backup data is automatically transferred offsite and is secured using FIPS 140-2 certified encryption technology via Private or Public Cloud – traditional backup architecture requires manual involvement when transferring data offsite on disk or tape and is thus not secure or reliable.

HIPAA Compliance and Confidentiality of Patient Data.

Any healthcare provider, healthcare clearinghouse, or health plan that electronically transmits or maintains health information pertaining to an individual must comply with HIPAA regulations. HIPAA impacts all areas of the healthcare industry. It was designed to improve the efficiency of healthcare by standardizing the exchange of administrative and financial data, and to protect the privacy, confidentiality and security of private medical information.

A major focus of all medical organizations is the security and privacy of electronic health records and their transmission between healthcare entities. Organizations must ensure the confidentiality and integrity of their members' health records, and transmission of data must be authenticated and encrypted. Additionally, security policies and procedures must be documented and implemented.

HIPAA's Security Standards is requiring healthcare providers to have a contingency plan to respond to any type of computer emergency. According to the latest rules published as of February 1, 2003, Asigra complies with the following HIPAA requirements:

- User Authentication.
- Role-based access.
- Encryption of data (AES 256 encryption).
- Offsite data storage.
- Transmission Reports.

Financial.

Technological advancements have improved the way financial service companies do business, improving transaction speed and efficiency. With these advancements comes more financial data than ever, and an even greater need to protect it from man-made and natural disasters.

New rules like Sarbanes Oxley, Gramm-Leach-Bliley and others, all developed to regulate the handling of financial data, have made it challenging for businesses to ensure they are protecting their data properly. Asigra helps financial institutions in complying with these legislations by doing the following:

- Storing data encrypted using 256-Bit AES encryption at all times at highly secure offsite data center locations.
- Performing disk-to-disk backup and retrieval of data.
- Creating an audit trail of all backups and restores.
- Restricting login privileges to administrative credentials only.

Gramm-Leach-Bliley Act.

This legislation includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule, and Pretexting provisions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities.

Sarbanes-Oxley Act.

SOX Act legislates how -- and how long -- companies can store their financial records. SOX safeguards against illegal financial activities by specifically stating that electronic records and messages, including email and instant messages, must be saved for at least five years and must be easily obtained if need be.

Asigra addresses SOX rules by keeping critical data secure, yet quickly accessible. The data is transmitted and stored in encrypted format, and remains in an encrypted vault where it is protected from unauthorized access or destruction.

To get more details on Asigra v9, click on www.RecoverYourCool.com/v9query to enter in your question and a product representative will get back to you.

About Asigra.

Leading organizations reduce costs by applying cloud computing to backup and recovery with **efficient**, **cost-effective** and **transformational** solutions from Asigra. Customers consistently redirect savings derived from our approach to projects of higher strategic and personal value, many of which have been on-hold for a year or more. The positive business outcomes made possible from a low-touch agentless architecture are revealed through Asigra's Day One ROI™ - an exercise that delivers enormous value with little up-front investment.

Tel: 416.736.8111 Fax: 416.736.7120 Email: info@asigra.com

RecoverYourCool.com