



Asigra Cloud Backup™ and Recovery Software.

Already Cloud Ready

Unprecedented data growth is challenging companies of all sizes, placing increasing pressure on their backup and recovery initiatives. With mounting pressure to comply with regulatory requirements and improve disaster recovery practices, companies are experiencing dissatisfaction with traditional backup methods that are falling short regarding efficiency, reliability, and ease of use. An ever expanding network of central, remote and branch offices further confounds the situation. The need to deliver against strict service level expectations, while managing costs, turns information recovery management into a complex challenge for enterprise data centers of all sizes.

With over 24 years experience, Asigra understands the challenge. We developed our agentless architecture in order to deliver an intelligent, elegant, yet easy to implement and simple to use solution with the most robust feature set on the market.

Asigra empowers your enterprise:

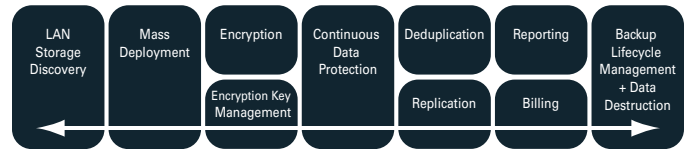
Data Protection Strategy: You do not need to choose whether to completely manage the entire company data or completely outsource it to an Online Backup Service Provider. Asigra is the only solution available that allows mixing and matching and seamlessly switching between the two strategies without having to reinstall the backup and recovery client software.

Public and Private Cloud Data Protection Strategy: You can leverage the Public Cloud or use your company's Private Cloud to optimize the backup of distributed remote locations, virtual machines and mobile users.

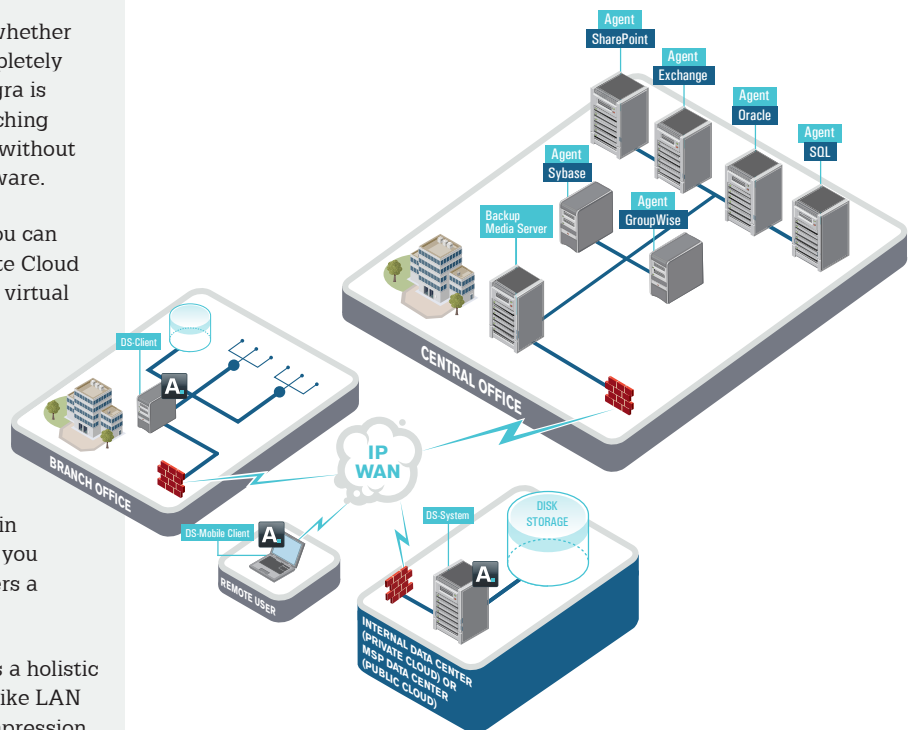
Control vs. Custody: Asigra is the only solution that always ensures your control of backup data. You can easily migrate your backup data from your internal data center to an MSP's facility or vice-versa, without having to reinstall the backup and recovery client software. As your backup strategy changes, retain the custody of your data or outsource it to an MSP, but you always have control over your backup data. Asigra offers a variety of clear, cloud-migration paths.

Single code base and common platform: Asigra offers a holistic data management solution that includes technologies like LAN Storage Discovery, Mass Deployment, Encryption, Compression, CDP, Deduplication, LAN Resource Discovery, Replication, Backup Lifecycle Management with a single code base and unified platform.

Asigra: Single code base and common platform



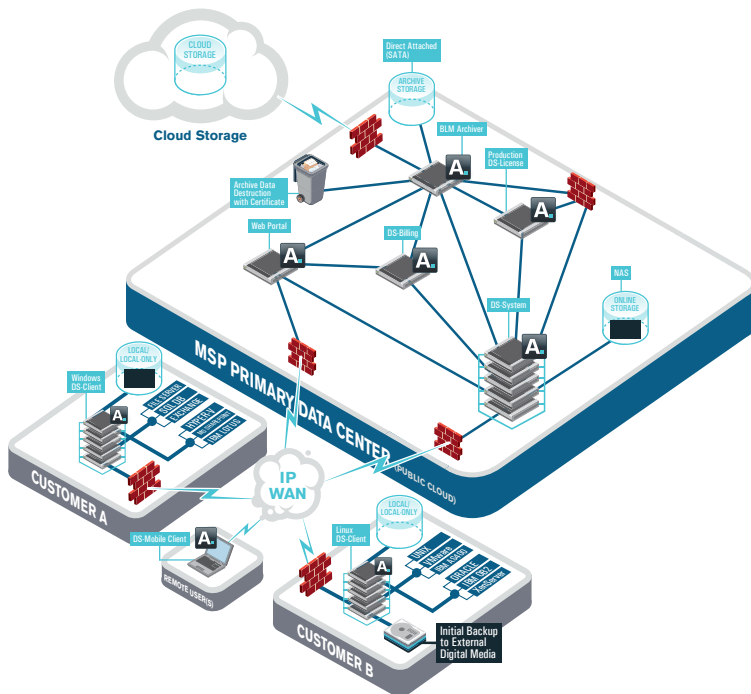
A new industry paradigm shift around backup redesign is finally catching up with virtualization and public/private cloud computing. Delivered to both small and medium enterprises (SMEs) and large enterprises as a standard (Private Cloud) license, term (Private Cloud) license, or as an online (Public Cloud) backup service, the Asigra solution is designed to deliver against strict service level expectations, while managing costs.





Asigra Software Overview

Asigra's software is comprised of two major components: the DS-Client (one installed at the edge of the cloud) where data needs to be protected); and the DS-System (installed at the vaulting location, or core of the cloud where the protected data resides). This scalability enables Asigra to support additional backup loads and multiple Operating Systems, servers, databases, applications, and storage environments. While these features were developed with the storage needs of large businesses and enterprises in mind, our pay-as-you-grow licensing model—which is based on the amount of compressed and deduplicated data stored—makes the solution well suited to SMBs (Small and Medium Businesses).



Agentless Advantage

Asigra's unique agentless data protection doesn't just match the capabilities of agent-based technology— it exceeds them. And it does so by no small margin. Like agents, Asigra protects all files (visible and hidden), databases, email systems and mailboxes, all standard Unix (including Mac OS X), Linux, Windows, even Systemi Operating Systems. And it does all this by working remotely through the Operating Systems' and application's APIs. Asigra's agentless architecture assures that you experience no Operating System and application disruption or downtime for implementation or upgrades; no security risk because of an open agent port that can be hacked; no server cycles being wasted for agent software. While at the same time you enjoy flexible RPO, including CDP, with incomparably fast and flexible recovery.

Asigra provides agentless backup and recovery support for all leading applications and Operating Systems:

- VMware
- XenServer
- Hyper-V
- MS SharePoint
- MS Exchange Server
- MS Outlook
- MS SQL Server
- SAP
- Oracle
- DB2
- PostgreSQL
- Sybase
- Lotus Notes and Domino
- GroupWise
- MySQL
- Windows
- Linux
- Unix
- AIX
- Novell Netware, OES
- Mac OS X
- System i/Power 6

Significant savings

Even if agents from traditional backup and recovery vendors were free, an Asigra solution would still enable huge reductions in operating expenses through its:

- Auto-upgrade to new software versions and Hot Fixes engine
- Central Management GUI interfaces
- Scheduling and automation of tasks, etc.

Simple licensing

Simply purchase software the same as disk capacity— no license fees, no tracking, no overspending on site licenses— you only pay for compressed and deduplicated capacity consumed.

One piece of software to install, manage, upgrade

Asigra software even self-upgrades, so there is no time-consuming and administrative-resource-draining pushing of agents or updates out to hundreds or thousands of remote-site systems.

WAN/LAN/CPU resource conservation

Asigra software runs with negligible impact on servers, workstations, and laptops, eliminating the CPU-cycle hits associated with agent-based solutions.

Robust, hardcoded security

There are no agents to open hacker-tempting ports in the firewall.

Elegant scaling

While agent-based solutions compound complexity in rapid-growth environments, the Asigra agentless backup/recovery solution easily accommodates new capacity, new applications, new sites, and additional backup sources.



DS-Client

Installed on: Windows, Linux, Mac

Scalable architecture to Grid Configuration.

The DS-Client is designed to accommodate a range of heterogeneous network backup requirements, and transmit data securely to the DS-System onsite or offsite via an IP WAN. The DS-Client is "agentless": it does not need to be installed on the machines it backs up. DS-Client is typically given administrator privileges and will back up data that it is allowed to access. DS-Client software is not licensed (except the EULA). You may install as many or as few DS-Clients as needed. DS-Client software may run on a dedicated DS-Client machine or on an existing machine on the LAN that it needs to backup.

Mobile Family Suite

For: Laptops, Consumers, iphones/ipods, Tablets and Smartphones.

DS-Client interface is designed to cater to the needs of non-technical users and protect the data from their offsite.



Standalone DS-System

Installed on: Windows, Linux Scalable storage through the Extensible Storage functionality.

DS-System software maintains, manages and validates the online storage repository where the backed up data transmitted by DS-Clients is saved. A DS-System may be used to provide backup/restore services to one or more DS-Clients under the same account or under different accounts, when DS-Clients reside on Windows, Linux or Mac. The DS-System is typically located in a secure offsite hosting facility. The Storage Architecture for the DS-System may be Direct-Attached-Disk, SAN or NAS depending on the DS-System type.

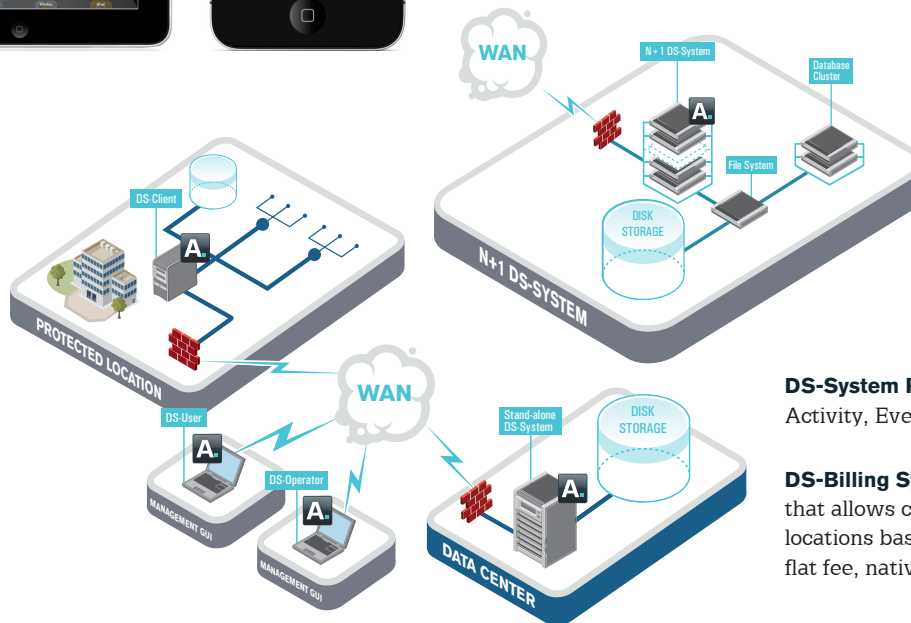
N+1 DS-System

Installed on: Windows, Linux.

Scalable architecture to more nodes in the N+1 and scalable storage through the Extensible Storage functionality.

The N+1 configuration of the DS-System is designed to allow for further scalability of the DS-System as well as to increase the availability of the backup service. It is designed so that the DS-System can survive failures for some of its nodes without interrupting the backup service.

An N+1 DS-System is made of several DS-Systems (denoted by "N") that work together to provide backup and restore services to the same DS-Clients. Any DS-System from the N+1 formation is able to provide any DS-Client with the same service (backup, restore, delete, synchronization, validation, etc.).



DS-System Reporting: Comprehensive Activity, Event, Audit Logs, and reports.

DS-Billing System: Separate Billing System that allows charging various business units or locations based on stored data, protected data, flat fee, native size or backup set types.

Replication DS-System

The Replication configuration of the DS-System allows storing backed up data into multiple geographical locations for redundancy and high availability reasons. Depending on the Replication configuration, DS-Clients can automatically fall back to replication DS-Systems for their backup, and restore activities if the main DS-System is not available. Replication DS-Systems can easily be turned into production DS-Systems by simply changing their license parameters. Replication DS-Systems are licensed separately.

DS-NOC

DS-NOC is a web interface that allows Enterprises or Service Providers to access and monitor DS-System, BLM Archivers or DS-Billing Systems remotely through web. Additionally, Service Providers use DS-NOC to enable web access for their end customers or partners to other DS-System, BLM Archiver reports, status updates, account/DS-Client creation on DS-System and web access to the archive data stored in the BLM Archiver. Users using the DS-NOC web interface have granular access to its functionality based on granted permissions. DS-NOC is licensed separately.

Backup Lifecycle Management (BLM)

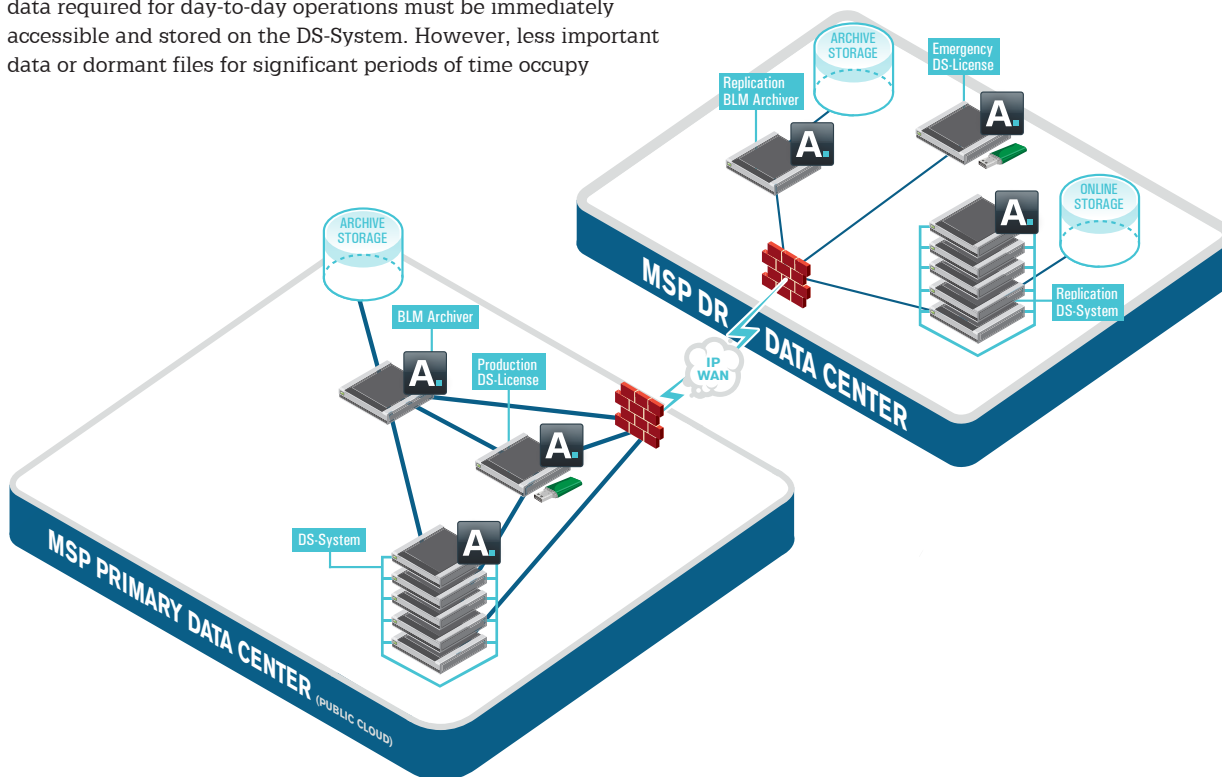
Every business stores data of varying importance. Mission-critical data required for day-to-day operations must be immediately accessible and stored on the DS-System. However, less important data or dormant files for significant periods of time occupy

premium real estate on the DS-System and should be saved to less expensive storage and eventually deleted to ensure compliance. The DS-System's online disk-based storage maintains critical data. BLM allows you to archive DS-System data for long term, either for cost or for regulatory compliance reasons.

- Saves money while still offering data protection by archiving obsolete generations and deleted data as well as old data.
- Enables compliance with backup regulations by allowing periodic copy archiving, and by providing data destruction (with certificate).
- Licensed per amount archived. Unlimited restores.
- It is a separately licensed piece of software.

Backup Lifecycle Management (BLM) Replication

The Replication configuration of the BLM Archiver is designed to accommodate replication data for one or multiple BLM Archivers for redundancy/compliance purposes. Replication BLM Archivers can be easily turned into production BLM Archivers by changing their license parameters and by reconfiguring DS-Systems to archive their data on the new BLM Archivers. Replication BLM Archivers are licensed separately.



Asigra Advanced Modules Overview

Modules are additional software functionality that may augment the core backup/restore capability of the DS-Client and DS-System. The modules are licensed separately, but are pre-integrated with the DS-System. Some of these are licensed separately.

Autonomic Healing

A veritable storage immune system, this module constantly scans the DS-System and immediately notifies when it encounters a corrupted or otherwise problematic file. Before the file can cause any harm, Autonomic Healing detects any corruptions (both data corruptions and logical inconsistencies caused by third-party technologies such as faulty RAID controllers, file systems, Operating Systems, disk subsystems, network packet loss, etc.) and sends notifications so that the personnel can fix the problem before it becomes harmful.

- Allows constant and seamless monitoring of DS-System storage.
- Saves time by identifying potential problems before they become serious issues.
- Ensures backup data is constantly in a valid state to maintain high SLAs for customer restores.

LAN Storage Discovery

This module completely analyzes the entire concentration of data on the LAN before you commit to a backup procedure. This module generates relevant reports that identify possible storage inefficiencies, thereby enabling you to optimize and better manage the backup procedure from both a data and cost perspective. Report data helps to show areas where you can:

- Increase server availability and performance.
- Isolate storage abuses before conducting a costly backup.
- Reduce backup window time.
- Optimize network disk space, which enables you to determine which files require backup.

Local Storage

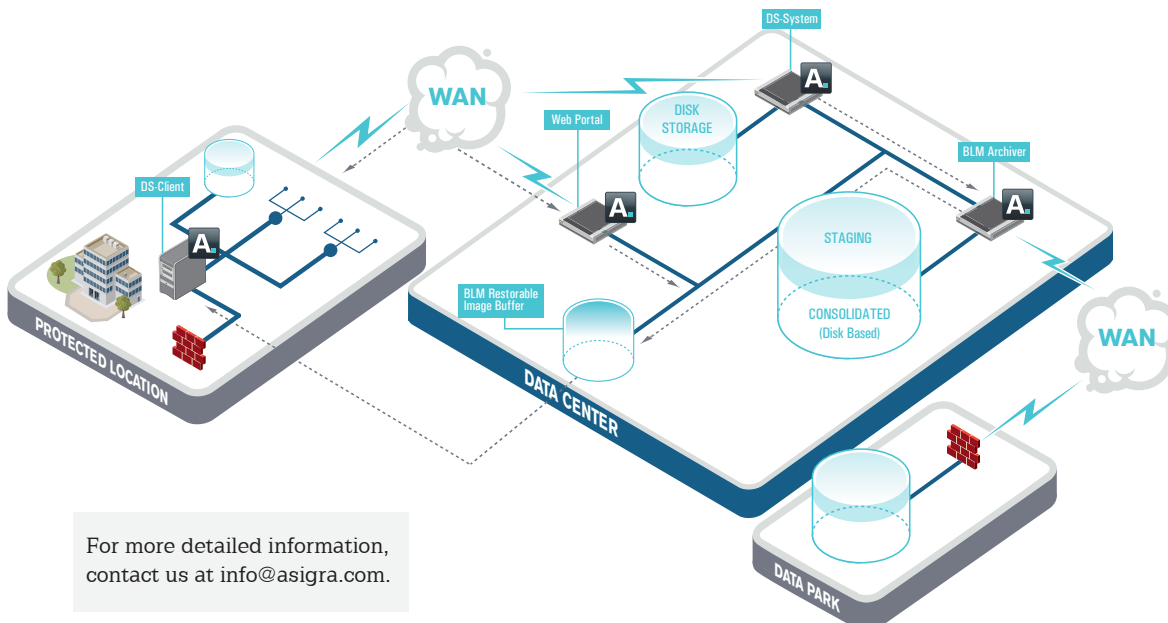
This module enables customers to store copies of their backed up data locally, on DS-Client LAN for fast restores in Disaster Recovery scenarios.

Local-Only

This module enables customers to store backed-up data locally only on DS-Client LAN. This module is capacity-based and is enabled from DS-System. It enables customers to specify data to be stored offsite and/or onsite or on-site only.

Other Modules

- DS-Recovery Tools
- Disc / Tape Module



For more detailed information, contact us at info@asigra.com.