

Agentless Architecture. Agentless Backup is Not a Myth.

Contents

The Agentless Architecture	2
Why This Matters	2
The Problem With Agents	4
How does it work?	4
Why it works?	5
The Benefits of Agentless: Reduced Costs, Robust Security, Simpler Scaling	6

Agentless Architecture.

Agentless Backup is Not a Myth.

The Asigra solution requires no agents, which inherently makes it easier to install and support than legacy backup and recovery solutions.

Backup and recovery software typically requires agents that are installed onto the host servers that a system administrator wants to back up. Even in a modest-sized environment, agent management can get extremely complex when an administrator is forced to deal with different operating systems and revision levels. The complexity of agent management is further complicated by the growing number of software packages that also require agents running on the same host servers, or what is also referred to as “agent pollution”.

Asigra does not require any agents to be installed but instead reaches out over the network to back up operating systems, file systems, and applications, using industry standard programming interfaces. To understand how Asigra backs up data over the network without the use of agents, consider how a local hard drive in a Microsoft Windows server can be backed up over the network.

A system administrator accesses the local hard drive over the network as a shared drive and maps it as a drive letter. A disk-to-disk backup of that hard drive can then be performed by copying the contents of one hard drive to another hard drive over the network. Asigra software works without agents but instead uses a sophisticated extension of this idea. This is simple and elegant in concept, but required a lot of hard work and years of development to get right on a broad variety of operating systems and data types.

Why This Matters

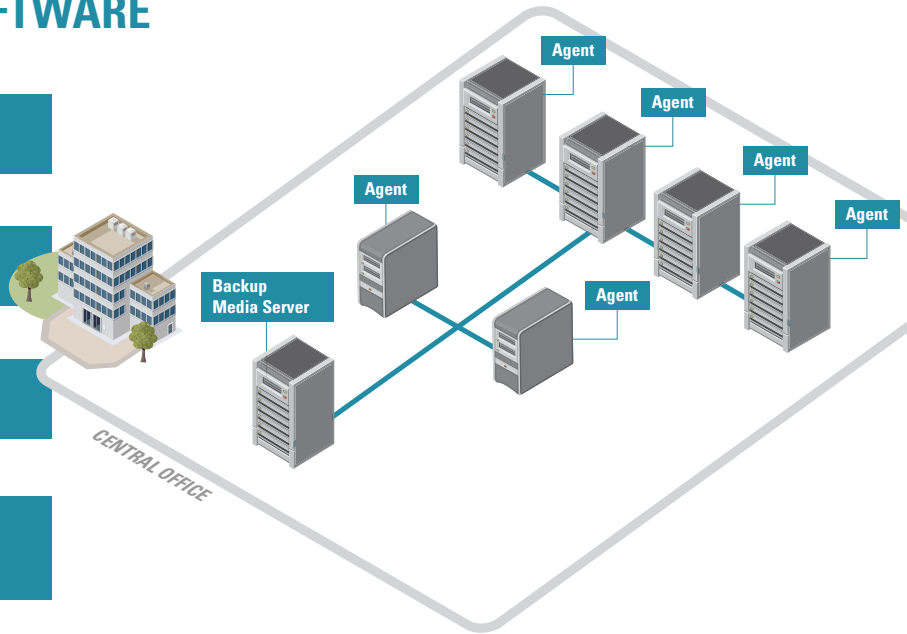
Dealing with backup software agents is a cumbersome and mundane task that can be extremely time consuming. Matching agent revisions with operating system levels, researching compatibility issues, and other labor-intensive tasks are non-existent when using the Asigra solution.

Additionally, many problems that occur while managing backup software are due to agent bugs and their incompatibility with

host servers. Asigra is inherently easier to support and the risk of problems is reduced as compared to other solutions because of its agentless design. Finally, traditional backup and recovery software puts agents onto servers and processing power is being stolen away from a server’s core application to feed the needs of agents. Asigra makes no such demands of the servers it is backing up.

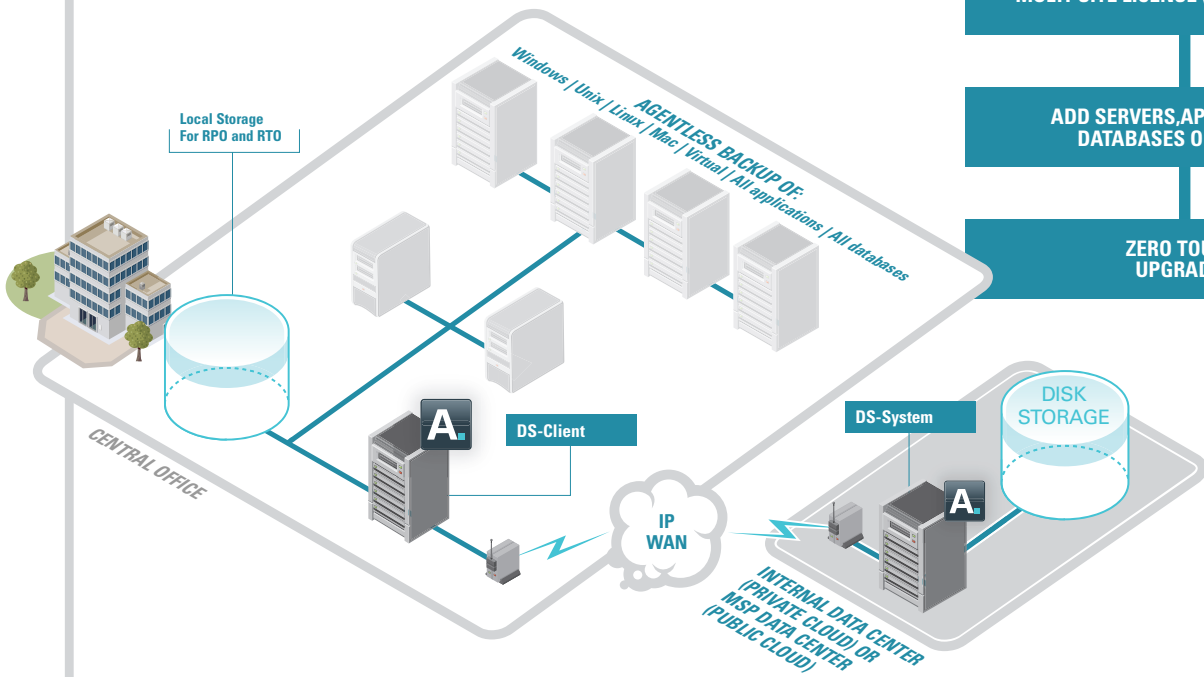
TRADITIONAL AGENT BASED BACKUP SOFTWARE

- Take the inventory
- Share it with the partner/vendor (Disclose network information)
- Ensure the configuration is accurate and buy the agents
- Buy additional agents when you add servers, applications, databases + upgrade all agents frequently



ASIGRA = AGENTLESS

- MULTI-SITE LICENSE (Capacity-based)
- ADD SERVERS, APPLICATIONS, DATABASES ON THE FLY
- ZERO TOUCH UPGRADES



The Problem With Agents

The presence of agents in the backup/recovery software (be it either a tape or a disk-to-disk (D2D) product), directly impacts data security, recoverability, and costs. IT managers already know the downsides that accompany agent-based solutions:

Compromised security. A port in the firewall must be opened for every agent. And, because almost every agent has administrative privileges, it effectively creates a backdoor hole in the server architecture—tap into the agent and have your way with the server. With no “in-flight” encryption mechanisms, agents also put data at risk during transmission from the remote office to the data center.

More pieces of software to manage and to fail.

More sites, more data, more applications, more users, more systems, more agents—growth makes everything harder to manage, and agents only compound the problem. As the infrastructure expands in size and complexity, problem diagnosis takes longer. Operating system upgrades, now implemented monthly by many organizations, have broader impact and potential to break software, including proliferating backup agents.

Agent management drains IT resources, causes disruptive downtime, and negatively impacts data recoverability.

Exorbitant licensing fees. Traditional software vendors charge for software based on the old per-system model, a pricey plan that requires customers to keep close tabs on

How does it work?

As the industry’s only agentless, multi-site backup and recovery software solution, Asigra technology completely eliminates the negative impact of agents. How does it work?

The Asigra architecture consists of two software components: the DS-Client and the DS-System.

DS-Client software, installed at the local or remote site on an existing or dedicated Windows, Macintosh, or Linux server, captures data from target backup machines. The DS-Client then conducts several data reduction processes, compresses, encrypts, and transmits the data via an IP WAN to the DS-System at the central location.

The DS-Client does not require installation of any backup agents

complex system and user landscapes. For many growing organizations, buying a site license is actually a simpler—albeit even more costly and often unnecessary—solution than trying to keep track of large numbers of backup products installed across hundreds or thousands of sites. There are even companies that now consult on doing audits to help enterprises try and lower license fees.

Mounting administrative costs. Heterogeneous application environments can be administrative nightmares when backup processes require the installation and management of agents for every single flavor of database, application and operating system platform. It takes time and a lot of ‘touching’ of remote-site systems to push agents and agent upgrades out to every server in the backup roster. And each time a data center administrator or service provider has to deploy an agent or intervene to support it at a remote site, that cost rolls back into their business model, making it increasingly difficult to be competitive or stay within budget constraints.

To put licensing and administrative costs in perspective, an enterprise with just five offices can easily spend \$50,000 to purchase and maintain the file/print server, email server, database, and workstation agents required for backup processes. For large enterprises with thousands of agents, licensing and support costs can quickly add up to millions of dollars.

on target servers, desktops, or laptops. The agentless DS-Client fully integrates with NT domains, Trusts and Novell NDS trees, and otherwise adopts the remote site’s existing LAN security settings. Using standard APIs, the DS-Client can remotely log in to target backup systems, capture requested data, and securely manage transmissions to the central site. Utilizing delta blocking and common file elimination technologies, the DS-Client reduces the amount of raw data transmitted and stored at the onsite or off-site vault.

The DS-System can be installed on Linux and Windows platforms and manages the online storage repository (configured as direct-attached disk, NAS or SAN) for backup data transmitted from one or multiple DS-Clients.

The Benefits of Agentless: Reduced Costs, Robust Security, Simpler Scaling.

Implementing an Asigra backup/recovery solution produces immediate and dramatic benefits. Compared to legacy agent-based alternatives, Asigra software offers:

Significant savings. Even if agents from traditional vendors were free, an Asigra solution would still enable huge reductions in operating expenses. As per an estimate, first-year operating expenses alone approach \$150,000 for an enterprise environment with 1,000 server agents. Annual server maintenance and operating expenses for this same configuration add up to nearly \$60,000. Eliminating agents eliminates those costs that are in addition to the purchase price of agents.

Simple licensing. DS-Client licenses actually ARE free. The DS-System offers businesses a unique pay-as-you-grow pricing model based on the aggregate amount of compressed data stored across the network. Simply purchase software the same as disk capacity—no license fees, no tracking, no overspending on site licenses—customers pay only for compressed capacity consumed.

One piece of software to install, manage, and diagnose. The 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. Delta blocking, common file elimination and compression technologies also minimize impact

on bandwidth and storage resources. While traditional agent-based backup/recovery solutions require implementation of high-speed pipes between the central data center and remote offices, Asigra enables the effective use of existing links such as DSL.

Robust, hardcoded security. Asigra software provides both 'in-flight' and 'at-rest' data protection, utilizing up to 256 bits for AES encryption keys to guarantee extremely safe data transfer and storage. And, it works within the organization's security framework—there are no agents to open hacker-tempting ports in the firewall. With secure data transmission across an IP WAN, the Asigra solution helps businesses achieve compliance, minimize information-loss liabilities, and protect customer confidence.

'Elegant' scaling. The DS-System is capable of elegantly scaling both in the dimensions of capacity and performance. This type of scalability is critical for environments with large numbers of remote sites, high-capacity data sets, and rapid high data growth. While agent-based solutions compound complexity in rapid growth environments, the Asigra agentless backup/recovery solution easily accommodates new capacity, new applications, and new sites. Features such as integrated loadbalancing ensure efficiency across multiple DS-System IP addresses.

Backup consistency, improved recoverability. The simplicity, efficiency, and security of the Asigra system promote implementation of consistent data backup programs across remote sites. Able to implement more frequent, successful backup processes, companies can significantly boost data recoverability in environments where success rates below 50% were once the norm.

Already Cloud Ready.

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

Asigra.