oncore IT

Call us
08451 489 248

Email us
sales@oncoreit.com

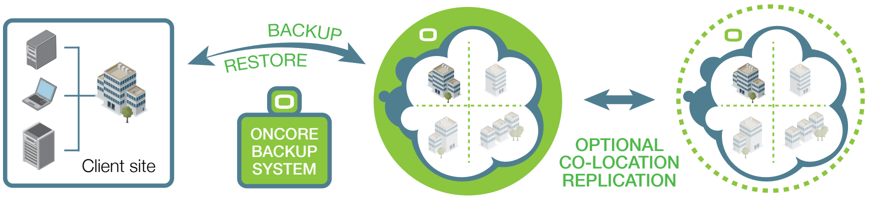
on backup

Easy, quick and cost effective data backup and restore you won't end up losing sleep over.

Backing up data is perennial headache. As information grows exponentially, backing it all up is complicated, time consuming and costly, with failure to do so opening up organisations to substantial business and compliance risk. Oncore IT, however, provides highly secure, simple to set up remote backup services using a best-in-class technology platform so you can safeguard your critical data against damage or loss.

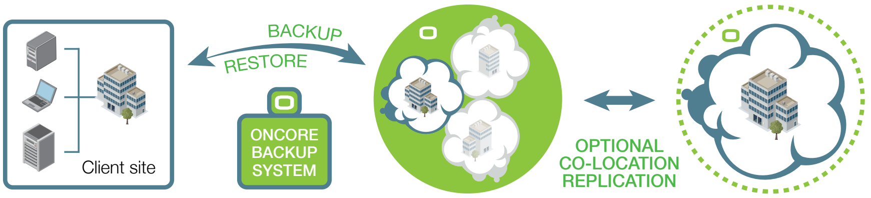
Asigra Vault Deployment Type

1 Public cloud



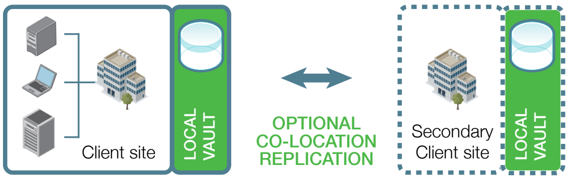
Multi-tennant
Shared Remote Vault
(Shared DS-System)

2 Private cloud



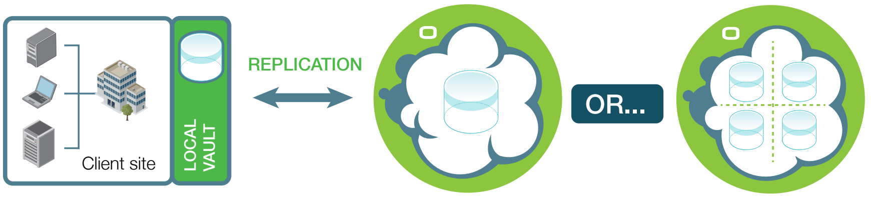
Single Customer Remote Vault/s
Single Customer Remote Vault from (own DS-System using Oncore IT License server)

3 Private vault



Single Customer Onsite Vault/s
Customer hosts their own Asigra servers & storage on corporate infrastructure with private Asigra license

4 Hybrid



Local Vault with Remote Replica
Customer hosts local vault with replication to the cloud (i.e. Oncore IT infrastructure). License back to Oncore IT servers.

Precise specifications may change without prior notice. E&OE.
This document does not constitute an offer for the sale of any particular product. All trademarks are acknowledged.

People who rely on their IT infrastructure rely on Oncore IT

Asigra Software Overview

Asigra software is designed from the ground up for the cloud and service delivery. Service oriented features like license management and centralized monitoring simplifies backup and restore management whether are you supporting a single department in an enterprise or thousands of customers on your public cloud. With deduplication and compression, network and storage usage is minimized and costs are reduced.

Asigra's wide range of support for common and not- so-common operating systems, servers, databases, applications, and storage environments ensures you can backup any environment however heterogeneous it maybe. While these features were developed with the storage needs of enterprises in mind, our pay-as-you-grow licensing model ensures you only pay for what you need.security including CCTV, biometric palm scanners, building monitoring and fire prevention.

Key Features and Benefits

Any Device, Application, Platform Support

- Physical and Virtual Machines
- Protect servers, desktops, laptops, tablets and smartphones
- Storage array snapshot support

Flexible Cloud Deployment

- Public/Private/Hybrid and flexibility to change models
- Address more market opportunities in enterprise
- Provide differentiated services

Multi-tenancy and Scalability

- Support thousands of clients and petabytes of data on an unified system
- Prevents cross contaminations of customer data
- Removes administration and data silos

Network and Storage Optimization

- Data reduction through deduplication and compression
- Incremental server backups and change block tracking
- Reduces WAN/network usage

Secure and Compliant

- 256-bit encryption
- Data encrypted in-flight and at rest
- FIPS 140-2 certified
- Meet regulatory compliance (e.g.SOX, HIPAA, BaselII)

Disaster Recovery

- Offsite replication and failover
- Backup and restore to secondary sites

Local Backup and Recovery

- Local backup option for fast backup and recovery
- Address tight Recovery Time Objectives (RTO)
- Self-service options to reduce management costs

Restore & Recovery Assurance

- Address varying Recovery Point Objectives (RPO)
- Bare metal, message level, and file level restore
- Data consistency and data transfer checks
- Autonomic healing
- Restore validation

Centralized Operations

- Web-based dashboard for centralized management/ monitoring
- Simplify deployment/management of remote customers

Asigra.

Key features

Block-Level Incremental Forever

Encryption FIPS 140-2 & Key Management

Deduplication

Compression

Continuous Data Protection

Validation Restore

Retention

Local Storage

LAN Storage & Resource Discovery

Reporting

Snapshot Support

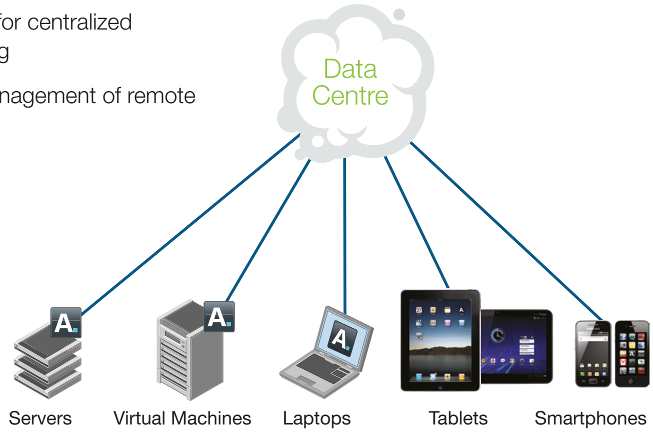
Replication

Extensible Storage

Autonomic Healing

Backup Lifecycle Management & Compliant Data Destruction

Billing Tier Storage



Precise specifications may change without prior notice. E&OE.
This document does not constitute an offer for the sale of any particular product. All trademarks are acknowledged.

Asigra Cloud Backup is comprised of three major components:

DS-Client

DS-Client software is installed at the end customer's premises where data needs to be protected. The DS-Client collects data from all machines, drives, applications and systems on the end customers LAN. The DS-Client software is agentless and does not need to be installed on every machine that needs to be backed up. DS-Client can run on a dedicated machine or on an existing machine on the LAN. It is designed to backup a heterogeneous environment of different OS, databases, applications, and data types.

DS-Client is offered in several variants:

1. Full-featured – for enterprise and data center backup
2. Mobile – for corporate managed laptops
3. Consumer – for consumer laptops and desktops
4. Smart phone – for corporate and consumer smart phones
5. Tablet – for corporate and consumer tablets

DS-System

DS-System software is installed at the enterprise or service provider's data center in the core of the cloud. The DS-System aggregates data from remote DS-Clients. The DS-System can leverage any disk-based storage such as be Direct-Attached-Storage (DAS), Storage Area Network (SAN) or Network-Attached Storage (NAS). The DS-System can be deployed as a stand alone or High Availability (HA) N+1 configuration.

The N+1 configuration is a redundant grid of nodes that provide further scalability, performance, and high- availability. This configuration allows the DS-System to withstand failures to up to half minus one the nodes in the cluster without interruption to the backup services. The addition of nodes also helps scale the performance of the grid by providing additional backup and restore processing resources.

DS-System also offers optional offsite replication for additional redundancy and Disaster Recovery (DR). DS-Clients can be configured to automatically failover to the replicated DS-System for both backup and restore activities. In prolonged outages, the replicated DS-System can be promoted to be the primary DS-System.

DS-Systems are offered in several variants and price points:

1. Full-featured – accepts connections from all variants of DS-Client
2. Mobile – accepts connections from DS-Mobile Clients for Windows and Mac, DS-Consumer, DS-Smart phone, and DS-Tablet Clients
3. Consumer – accepts connections from DS-Consumer, DS-Smart phone, and DS-Tablet Clients

Backup Lifecycle Management

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 backup data for long term, either for cost or for regulatory compliance reasons.

- Saves money while still offering data protection by archiving obsolete generations, deleted data, and old data
- Enables compliance with backup regulations by allowing periodic copy archiving, and by providing data destruction (with certificate)
- Offsite replication option for additional redundancy and compliance

Precise specifications may change without prior notice. E&OE.
This document does not constitute an offer for the sale of any particular product. All trademarks are acknowledged.