



Nexsan Assureon

The Nexsan Assureon is a storage solution for archiving that is delivered as an appliance with the hardware and software integrated into a complete, ready to install and use system. The Assureon has several models that vary in capacity and capability to meet archiving needs for unstructured data archiving. The original Assureon products were released in 2005 after the acquisition of the Montreal, Canada firm Evertrust. The current generation of Assureon systems was released in 2007. The Nexsan Assureon systems are targeted at archiving unstructured data across multiple industries and market segments with the capability to meet multiple regulatory and corporate governance requirements around records retention.

OVERVIEW

The Assureon system creates independent archives (repositories) for the archiving of information. The archives can have different retention policy settings and administrative controls to provide isolation of data. Standard servers and Nexsan storage are used in the systems, which are delivered as appliances. Unstructured files from application and file servers are archived as files and managed by the Assureon which internally creates an object that contains the file contents and a separate object that contains the file's metadata. The Assureon uses the digital fingerprint of the data as an internal reference within the Assureon. Using the digital fingerprint is called Content Addressable Storage (CAS) by Nexsan. The Content Address is not exposed to the application or to standard file access.

The digital fingerprint is called uFID and is created by the application or file server or the Edge NAS controller where the file is written. The uFID consists of the following information that is combined:

- 128 bit MD-5 hash across the file for a sequence of 32 hexadecimal digits
- 160 bit SHA-1 hash across the file for a sequence of 40 hexadecimal digits

The metadata created and associated with the file is digitally signed, time stamped, and stored separately from the file object. Each instance of the same file content results in its own metadata file that includes the:

- File name and size of the file sent to the Assureon
- A signature ID which is a globally unique serial number assigned to the file by Assureon
- The original source of the file – domain, server name, and path
- Dates the file was created, modified, and last accessed
- A time stamp for when the file was archived
- Digital fingerprint (uFID)
- Encryption key ID (if encryption is enabled)
- Retention policy associated with the file including the retention date and do not delete before date
- Uniform Resource Identifier if applicable

The metadata is also stored in a Microsoft SQL database which may be used in searching through the Assureon SysAdmin Web GUI.

The archiving functions are detailed in the Advanced Features section of this document. These features enable the security, retention management, and availability needed by enterprises for an archiving system.



Nexsan Assureon

HIGHLIGHTS

- Archiving system delivered as appliance using standard server hardware with Nexsan storage and custom software running on a locked-down Windows 2008 server system.
- Different Assureon Models for different usage cases. All configurations will make at least two copies of data that can be either local or remote.
 - SX – Single site, single node Assureon with up to 28TB of usable capacity
 - SXR – Replicated Assureon nodes with one local and the other remote with up to 56TB of usable capacity per node (with single copy at each of two sites)
 - NXR – Replicated Assureon appliances (one at both sites) with 2.7TB of usable capacity and native CIFS and NFS support with the integrated Assureon Edge NAS
 - AXR – Replicated Assureon appliances (one at both sites) with 3.8 TB of usable capacity
 - HXR – Local Assureon system connected to a hosted (cloud service provider) Assureon for the second copy. Up to 56TB of usable capacity per node. NHXR and AHXR are hosted appliance versions of the NXR and AXR. One copy is made locally and the second copy is in the hosted cloud service provider storage.
- RAID 6 disk storage for SX, SXR and HXR
- RAID 5 disk storage for NXR and AXR
- Scalability with addition of nodes and automatic system expansion
- File ingestion options
 - Assureon Client archives data directly from file systems on Windows 2003/2008 servers
 - Assureon NAS controllers (NAS head) with CIFS and NFS interfaces
 - The NXR model includes a native Edge NAS controller
 - Intermix of Assureon Clients and Assureon Edges
- Retention control settings – policies and retention length
 - Two types of retention:
 - Guaranteed retention – retention period can be extended but not reduced
 - Flexible retention – can set minimum and maximum and allow retention period to be extended or shortened with boundaries
 - Configurable retention settings by application, directory, file types, and other selectable file granularities
 - Last access time override (NetApp SnapLock method)
 - XML ingestion file
 - Application software access over Ethernet using custom Assureon API to set retention period
- Security and compliance features
 - Single or multi-tenancy support with logical physical separation
 - File-by-file encryption using AES256 encryption with key management service
- High availability using custom clustering software
- Automated retention and deletion policies and enforcement
- WORM emulation in software and storage firmware
- Optional full-text indexing and search with addition of Assureon Content Search node (server) and COVEO Enterprise Search software
- Remote replication to the other Assureon node(s) for protected copies
- Ethernet and optional InfiniBand connection for access



Nexsan Assureon

PRODUCT ARCHITECTURE

The Nexsan Assureon is a software implementation for archiving of data that runs on standard servers with Nexsan storage. The software features are extensive (described in the Advanced Features section of this document) for archiving to meet corporate governance and regulatory compliance requirements. The underlying operating system is a locked-down version of Windows Server 2008 which does not allow native access to install additional software or for administrators to modify.

Using standard server hardware with Nexsan storage, the Assureon is delivered as an appliance where the software is pre-installed and the system is ready for network attachment and archiving of data. To meet different price points and functionality, Nexsan provides different Assureon models with different capabilities. Currently, the available models are detailed in the following diagrams and explanations.

SX – The SX is a scalable single site, single node system with disk capacity of 3 to 28TB based on the drive size used, the average file sizes to be archived, and the number of disks in the attached SATABeast or SATABoy Nexsan RAID systems. Two copies of data are always written at the single site. The SX uses a controller which is a Dell server with the Assureon software installed and either SATABeast or SATABoy disk storage systems attached. The disk storage systems have special Assureon firmware functions enabled. A controller can have up to four disk modules attached. Because two copies of data are always made, with the SX system, the usable capacity is always $\frac{1}{2}$ of the disk storage attached. The pairing of the controller and the storage system (SATABeast or SATABoy) is called a “brick” and capacity scales beyond the disk modules by adding complete bricks (additional Assureon systems).

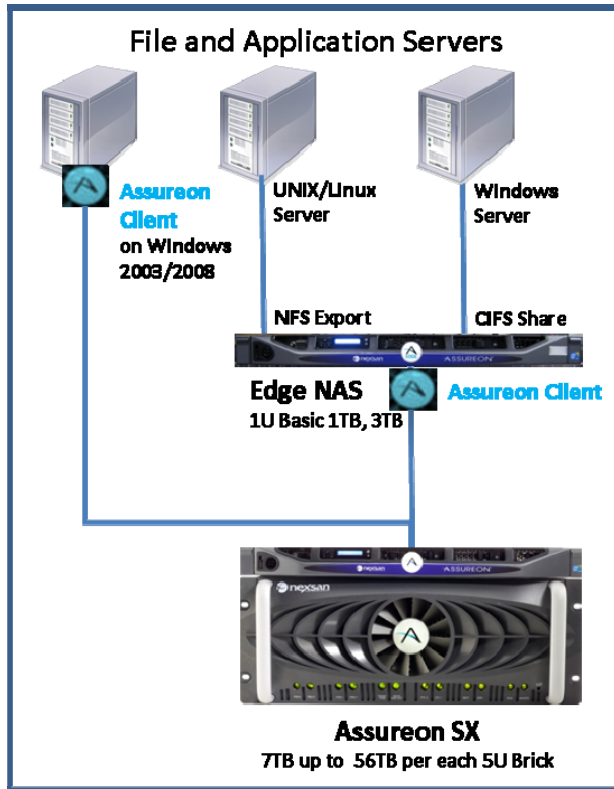
An SX brick includes four SAS drives for the operating system and database. Additional drives and arrays are for the archived data. SATABeast-based storage configurations include two SATA drives for cache in addition to the arrays of disks for archive storage.

The SX receives data from either an Assureon Client on a Windows 2003/2008 application or file server or an Assureon Edge which is a NAS system that serves files for NFS and CIFS access. The Edge will have the Assureon Client installed (previously called FSW or File System Watcher). The Assureon Client will monitor the files stored in archive directories on application or file servers or the Assureon Edge NAS and based on policy settings can perform the following actions:

- Archive and shortcut – move the file to the Assureon and leave a shortcut in its place. It can also archive and insert the shortcut after x days where x is a policy based setting of creation date or modification date are x days old.
- Archive and leave – move a copy of the file to the Assureon but leave the file on the file server
- Archive and delete – move the file to the Assureon and delete it from the file server

The Nexsan Assureon Edge NAS can have variable amounts of capacity attached as a file server and can optionally be connected to the Assureon using InfiniBand to increase the bandwidth for file ingestion. The Edge Basic comes with 1TB or 3TB of internal storage. The Edge Advanced is diskless and paired with an Assureon SATABoy or SATABeast for a variable amount of capacity. The following diagram illustrates the SX model.

Nexsan Assureon



Assureon SX system includes one brick (2 copies of the data within the brick).

1. Assureon Client migrates files from Windows 2003/2008 servers to Assureon according to policies.
2. Optional Nexsan Assureon Edge NAS with file system access via CIFS and NFS. Includes the Assureon Client.
3. Assureon manages the archive and the protection and retention of file

Figure 1: Nexsan Assureon SX Usage

The SX models and capacities are listed in the following table:

Model	Usable Capacity	Disk Type	Storage System
SX-7	7 TB	1 TB SATA	SATABeast
SX-14	14 TB	1 TB SATA	SATABeast
SXL-14	14 TB	2 TB SATA	SATABeast
SXL-28	28 TB	2 TB SATA	SATABeast
SX-3	3 TB	1 TB SATA	SATABoy
SXL-6	6 TB	2 TB SATA	SATABoy

Table 1: SX Models

Nexsan Assureon

SXR – The SXR is the redundant, high availability configuration of the SX model. With the SXR, a second SX system is used which may be in a remote location. The SXR will automatically replicate data between the Assureon systems over Ethernet. The replication may be bi-directional from independent archives on the SXR.

Because there are two copies of data made by the Assureon with the SXR, one copy is made locally and the second is remote. This allows the capacity of the local system to be equal to the installed usable disk capacity. The second copy is on the remote system which has the same usable capacity. The capacity for the SXR can scale up to 28TB or 56TB.

The following diagram illustrates the SXR model and highlights access from servers at the second site. The system can scale with addition SXR systems added at both the local and remote sites.

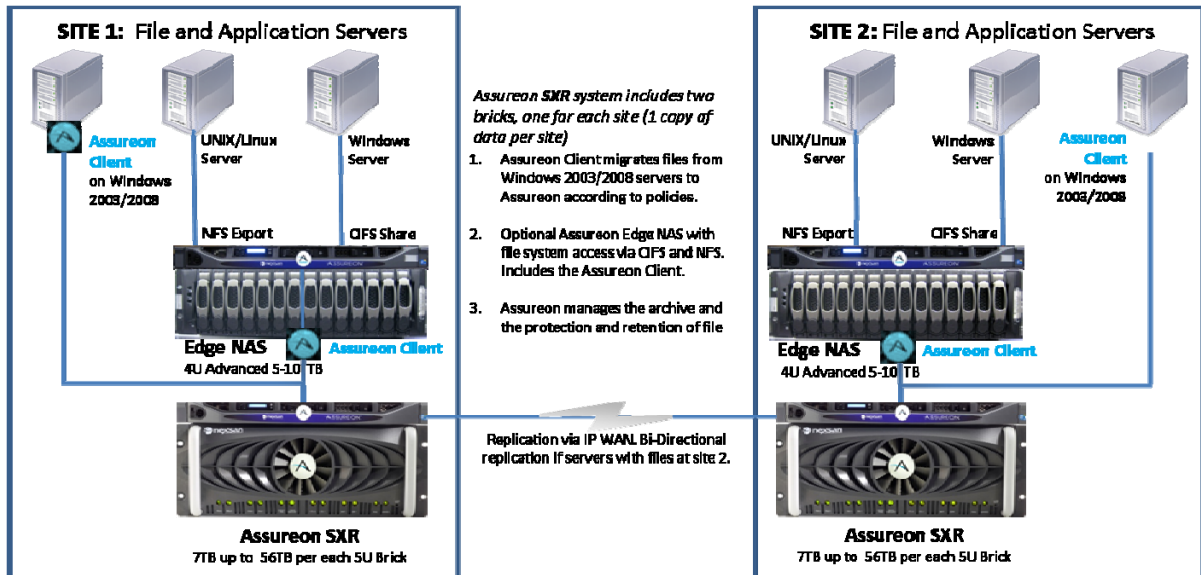


Figure 2: Nexsan Assureon SXR Usage

The SXR models and capacities are listed in the following table:

Nexsan Assureon

Model	Usable Capacity	Disk Type	Storage System
SXR-7	7 TB	1 TB SATA	SATABeast
SXR-14	14 TB	1 TB SATA	SATABeast
SXR-21	21 TB	1 TB SATA	SATABeast
SXR-28	28 TB	1 TB SATA	SATABeast
SXRL-14	14 TB	2 TB SATA	SATABeast
SXRL-28	28 TB	2 TB SATA	SATABeast
SXRL-42	42 TB	2 TB SATA	SATABeast
SXRL-56	56 TB	2 TB SATA	SATABeast
SXR-3	3 TB	1 TB SATA	SATABoy
SXR-8	8 TB	1 TB SATA	SATABoy
SXRL-6	6 TB	2 TB SATA	SATABoy
SXRL-16	16 TB	2 TB SATA	SATABoy

Table 2: SXR Models

NXR – The NXR is a replicated Assureon appliance with a fixed amount of capacity where the disks are contained within the controller. The NXR can have 2.7TB of usable capacity. Because two copies of data are made, there is actually twice as much disk in the Assureon system. The NXR differs from the other models in that the NAS function is embedded in the NXR model for NAS access using CIFS or NFS. It does not require a separate NAS system as with other models. The NXR also includes additional Assureon Clients to ingest files from other Windows servers. The following diagram illustrates the usage of the NXR model.

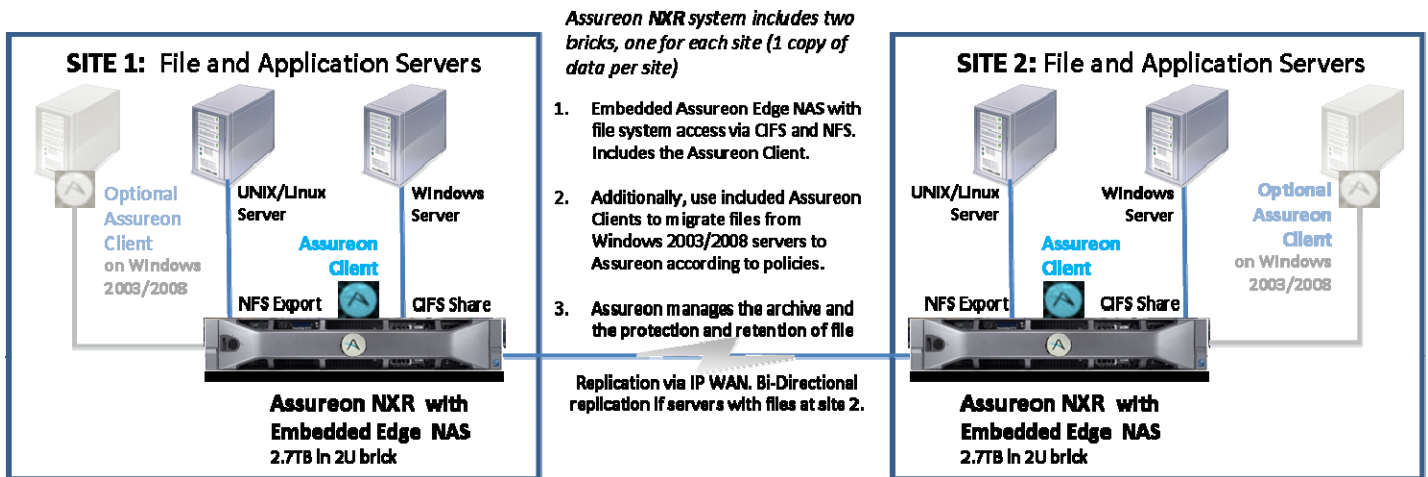


Figure 3: Assureon NXR Model Usage

AXR – The AXR is a replicated system with a fixed amount of capacity where the disks are contained within the controller. The AXR is the same system as the NXR except it has 3.8TB of usable capacity and

Nexsan Assureon

it does not include the NAS feature capability. The AXR can ingest data directly from Windows 2003/2008 servers with the included Assureon Clients. Optionally, an Assureon Edge NAS controller can be added to provide NFS and CIFS access. The following diagram illustrates the usage of the AXR model.

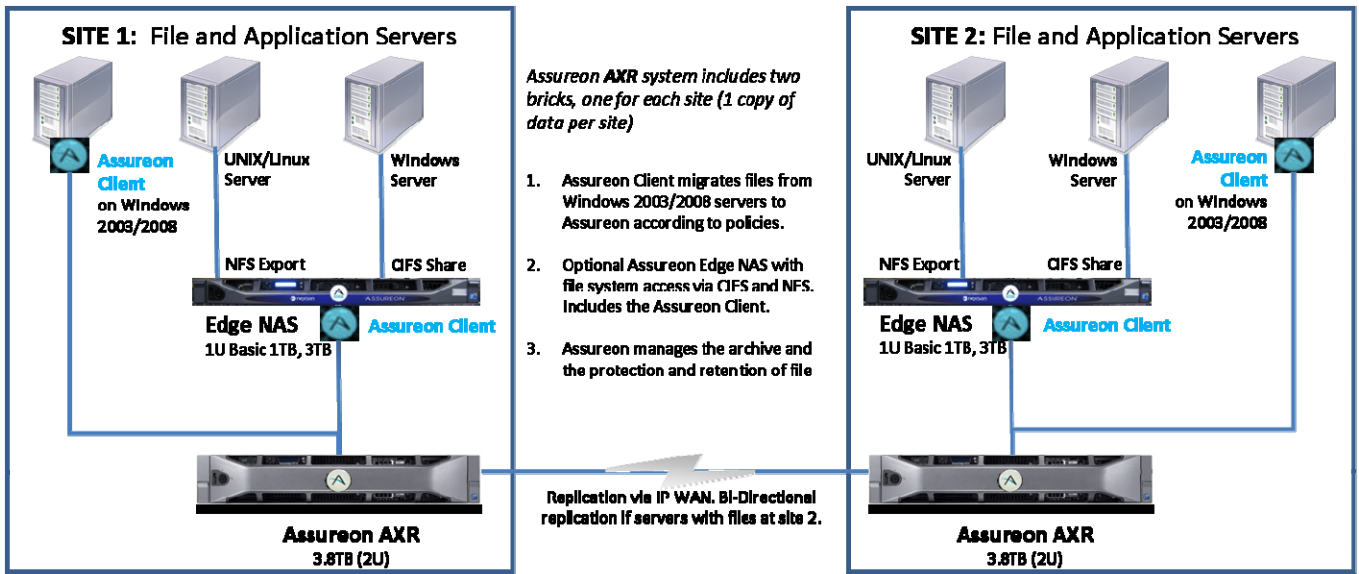


Figure 4: Nexsan Assureon AXR Model Usage

HXR – The HXR is similar to the SXR system except the second copy of data is to a hosted facility – which may be service provider / cloud facility. There is no difference with a standard system other than the second copy of data is stored remotely. The following diagram illustrates options for using the Assureon models in the mHXR configuration where one system is at the customer site and the second system and copy of data is at a service or cloud provider facility.

Nexsan Assureon

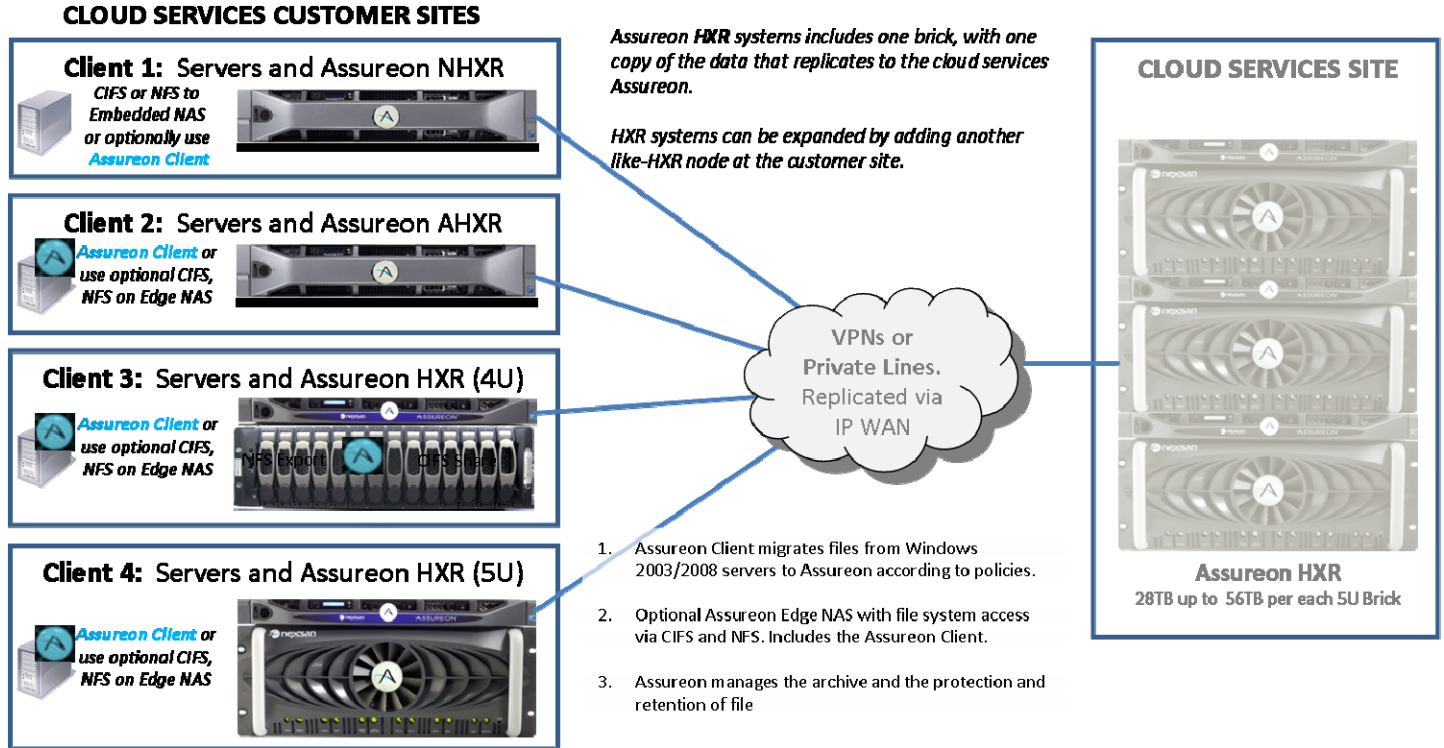


Figure 5: Nexsan Assureon HXR Model Usage

Evaluator Group Comment: It should be noted that for additional capacity multiple Assureons are expected to be used. We think many customers would prefer the option to scale the systems much larger and maintain a single system for practical purposes. A single system that scales larger may also be much less expensive than multiple systems but may not have the aggregate bandwidth required.

Hardware

The hardware used in the Assureon consists of standard servers (from Dell) and Nexsan block storage systems. Delivered as a complete system with the Nexsan software pre-loaded, the servers are labeled as Nexsan Assureon systems. The Nexsan storage systems used are the same block storage systems offered as independent storage with one additional feature enabled for the Assureon. The storage has a special “lock-down” mode that prevents deletion or modification of RAID sets, LUNs, and other configuration options in order to maintain the integrity required of storage for an archiving system.



Nexsan Assureon

There is no architectural limit on the capacity but the systems are delivered with set capacity amounts. The maximum number of nodes that can be configured for some models is only limited by the number of tested configurations that are allowed.

By using Dell servers for the Assureon controllers, Nexsan does not need to invest in the ongoing development for the controller. The servers continue to change with new models so the actual specifications of the controller (servers) will change with frequency of the server change. The current Dell server specifications should be consulted for the controller detail information. An optional hardware feature is an InfiniBand connection using HCA's for high bandwidth file access. With InfiniBand usage, the Assureon would typically be connected from the Assureon Edge or a Windows server via InfiniBand.

By using the standard Nexsan storage system, the Assureon can take advantage of the automated spin-down feature for the disk drives. Termed "AutoMAID," the spin-down of disks is granular to a drive or RAID set level.

The Nexsan AutoMAID (Massive Array of Idle Disks) has a multi-level implementation which can trade-off the power savings compared to the time to access data. Based on no host access for a selectable period of time, the settings in the Nexsan storage system can be:

- **Level 1:** Heads Unloaded
 - 15% to 20% savings
 - Sub-second recovery time
- **Level 2:** Heads Unloaded, slows to 4000 RPM
 - 35% to 45% savings
 - 15 second recovery time
- **Level 3:** Stops spinning (sleep mode; powered on)
 - 60% to 70% savings
 - 30 to 45 second recovery time
- **Level 4:** Entire RAID group stops spinning.

The Assureon connected storage is installed with Level 1 as the default option. The customer may enable other levels based on their needs.

Nexsan Assureon



SXR
7-56TB
(5U per Site)



SXR
3-16TB
(4U per site)

Assureon System Elements

- Additional Assureon "Bricks" are added to expand capacity. Bricks combine the processing and storage node.
 - › NXR's expand with added 2U NXR bricks
 - › AXR's expand with added 2U AXR bricks
 - › SXR's expand with added 4U or 5U SXR bricks



NXR 2.7TB with NAS or
AXR 3.7TB without NAS
(2U per Site)

Figure 6: Nexsan Assureon System Elements (Source: Nexsan)

Software

The archiving software is custom software running on Windows Server 2008 operating system. The Windows system is locked down such that additional programs cannot be added, modifications to the system may not be done, and unneeded services are disabled. A Microsoft SQL database is used for metadata and other system control information.

High availability is accomplished with clustered software where a node that fails can be taken over by another node in the cluster. The clustering software was developed for the Assureon and supports active-active operation between nodes for read failovers and active-passive for write failovers. Assureon also has the capability to have multiple nodes for system scaling, and load sharing between nodes.

Evaluator Group Comment: Using Windows Server 2008 in a locked down mode as the underlying system is a very smart move for Nexsan. By doing so, the Assureon has a native CIFS implementation and integration with AD. Given the fact the majority of the markets for archiving data are Windows environments, they have met major requirements. This also allows Nexsan to leverage the R&D investment in Windows Server while spending their own development dollars on the archiving functionality.

Nexsan Assureon

Vendor	Nexsan
Product / Version	Assureon
Environment	
Usage Environments	Windows, Unix/Linux, Apple MacOS
Supported files / capacity	No architectural limit
Removable media	No
Admin Interface	WebGUI, role-based admin
Remote replication	Yes - WAN-based
System access	NXR Model: embedded NAS - CIFS, NFS AXR, SX, SXR, HXR Models: w/optional Assureon Edge NAS. Opt InfiniBand
Custom API required	Not required but can use as alt method to set retention
HA available	Yes
Security Access	AD, ACLs, certificate auth.
Operational	
Storage technology used	Nexsan RAID disk systems, integrated disk (AXR, NXR), or cloud
Integration with software	No
System logging	Yes
System automatic reporting	Yes
System self-protecting	Yes - requires remote system
Compliance Functions	
e-Discovery: content indexing, search, export	No - separate server and COVEO software
Automatic copies	Yes - makes two copies on disk - local or remote

Unique copy serialization	Yes
Multi-tenancy - isolation to storage devices	Yes
Secure delete	Yes
Legal hold on files - multi-overlapping	Yes, Yes
WORM	Yes – by software & stg firmware
Multi-regulations simultaneously	Yes
Audit-trail with chain of custody for data accesses	Yes
Integrity check on retrieval	Yes
Retention controls - default setting by archive	Yes
Retention controls - application controlled setting	Yes - with API or Last Access override
Retention controls - automated actions on expiration	Yes
Write verification	No
Advanced Features	
Power - auto spin-down of disk drives	Yes
Containerization	No
Single instancing	Yes
Compression	Yes for text files
Encryption	AES-256, FIPS 140-2, automatic key management
Versioning	Yes
Archive media recycling for reuse	N/A
Media consolidation	N/A
Reconstruct lost media	N/A
Reporting	Yes - extensive

Table 3: Assureon Specifications



Nexsan Assureon

RELIABILITY, AVAILABILITY AND SERVICEABILITY

The availability of the Assureon depends on whether the model is a single site or replicated system. Replicated systems have the capability for failover and failback in case of a node failure either locally or remotely. Read failovers are automatic while write failures are manual operations. In addition, the systems maintain two copies of all data, four copies of the internal database, and the ability to bi-directionally, remotely replicate information to another Assureon for disaster protection.

Other RAS characteristics include:

- Two copies of data are made to different disks in single site systems. Replicated systems make one copy locally and one copy remote.
- Redundancy of active components including fans and power supplies on servers and storage systems
- Multiple Ethernet port access to HA systems
- Redundant key servers and a remote key server capability
- Error notification and logging
- System monitoring of thresholds, events, client access, and file integrity
- RAID 6 is used to protect from failure of two disks in a RAID array
- Periodic check of the integrity of the data is performed using the digital fingerprint. If a problem is found with the file, the file is quarantined and replaced with the alternate copy to repair the integrity of the data.



Nexsan Assureon

ADVANCED FEATURES AND FUNCTIONS

As an archiving system, the important features are different than traditional disk-based storage systems. The focus for the features is on the archiving and retention management capabilities. The following are how the features are addressed by the Assureon system.

Retention Management – Archived files can have retention settings inherited from the archive where they are stored. Retention settings can also be established by an administrator for the types of data being archived. There are two forms of retention: Guaranteed Retention where the retention period can only be extended and Flexible Retention where minimums and maximums are set and the retention period can be modified within those boundaries. The retention policies are set at the directory level for the source data. An application can also set the retention controls for an individual file based on a custom API. Assureon also permits an overload of the Last Access time before the R/O attribute is set to establish the retention period. This is the same method as used in the NetApp SnapLock implementation.

Immutability – An archive can have all files set into WORM mode (write once read many) for immutability meaning that the file cannot be altered or erased. The immutability applies until the retention period expires at which time the file (and its metadata) can be deleted. The WORM setting is enforced in the software and with special versions of the embedded code on the Nexsan disk storage.

Security: Tamper Protection and Administration Access – The Assureon uses Smartcard tokens for *authentication* for administrator access. There is also an *audit* trail log kept for all administrator *access* and actions. IPsec is used for network security of data. There are multiple levels of security for control of administrative and management access. Nexsan provides a service for a secure timestamp. The subscription service allows an Assureon to receive a secure timestamp to apply to files for retention purposes. This prevents circumventing the control of retention access by resetting the Assureon system clock.

Security: Access Protection – *Authorization* of access to documents is required and the Assureon uses Active Directory, certificate authorization, or manual control of *access* with userids and passwords through the administrative interface. An audit trail of access to documents is maintained. Currently, the Assureon does not do NTFS permission inheritance.

Encryption – Data encryption is an option for all stored data. AES-256 encryption is used for each file individually. Encryption keys are managed by an encryption key server with both a local and a remote key manager. Nexsan provides the key management as a subscription service along with the timestamp service. Clear text keys are not transmitted – only encrypted encryption keys are sent to the remote key servers in two locations. The encryption has FIPS 140-2 certification which is required for governmental usage. In addition, for media that is offline such as tape or optical disk, when data is deleted the encryption keys are destroyed so data cannot be recovered and the media does not need to be recalled for deletion. The Assureon uses the Intel crypto processor to accelerate the encryption calculation.

Compression / Single Instancing – The digital fingerprint used for data authenticity checking is also used for single instancing (file-level deduplication). Only a single copy of a file in an archive will be stored. There is no option for disabling single instancing. There is a data compression function within the Assureon system which Nexsan recommends using only for pure text types of files.



Nexsan Assureon

Legal Hold – Files in an archive may be put on legal hold by an administrator either individually, as a group within a file structure, or as a result of a metadata query operation. After a legal hold is applied, the file may not be deleted even if the retention period has expired. Once the legal hold is removed, the retention expiration actions may be performed if the file has met its criteria for the retention policy. There is no limit on the number of legal holds.

Multiple Copies – Two copies are automatically made when data is stored on disk. The second copy may be on a local system or on a remote system. There is an option to make two copies at each site.

Data Authenticity – As messages or files are ingested, the digital fingerprint called uFID is created on the application or file server or on the Assureon Edge. The digital fingerprint consists of a 128 bit MD-5 hash across the file, a 160 bit SHA-1 hash across the file, and the file length. The digital fingerprint is saved with metadata along with the file. The digital fingerprint is validated when the file has been received by the Assureon for archiving and again upon file retrieval, where the digital fingerprint is created again and checked against the original to assure the integrity of the document.

Evaluator Group Comment: *This is probably the most intensive integrity check of any archiving system. A single hash code would probably have been sufficient but the Assureon goes beyond to meet any demanding environment.*

Isolation of Data – Data can be physically isolated by assigning archives to specific storage. Multi-tenancy is supported from an access and an administration standpoint.

Archive Data Protection – Two copies of data are made on disk. Previously, the Assureon allowed attachment of tape or optical storage to make backup copies of the archive. That option is no longer available.

The replication to another Assureon over IP may be configured either as an active-active (bi-directional replication) or active-passive (one-way replication). For disaster protection and business continuance, the remote mirroring capability will provide the availability required.

Search – The search function is a separate server and storage from Nexsan with COVEO Enterprise Search software incorporated as the Assureon Content Search. Office files, PDF text file, HTML and text files are supported for content indexing. There is no integrated search capability included with the Assureon. The Assureon Content Search is done from a browser style interface with search controls so that documents can be searched by date, title, location, size, author, keywords, or phrases. The results of the search are excerpts containing the context and summarization with the query items highlighted. All results are deduplicated and have a quick feature so that cached version of the documents can be examined. User credentials are checked so that only the documents that the user is permitted to see are presented in the results.

Audit Trail (Chain of Custody) – A system log of changes is maintained by the Assureon including all retention control operations and an audit trail of access is also kept. A chain of custody report on individual documents can be generated which meets some regulatory requirements.

Data Shredding – There is a data shredding capability using digital overwrite of data option when a file is deleted.



Nexsan Assureon

Versioning – Versioning of documents where multiple versions of a document with the same name may be stored is supported by the Assureon. There is a configuration option for how many versions of a document to store or specifying a maximum number of versions for flexible retention policies.

Evaluator Group Comment: *There are some key features and capabilities that are expected in an archiving system which are not available or incomplete with the system. Some of these may be required for compliance or governance reasons while others are expected for some operations. These features are listed below.*

Write Verification – No write verification setting is available with the Assureon for disk storage.

Containerization – Containerization is not performed on files stored on disk in an archive. External applications must be used for containerization.

Export – No built-in export capability is available in the system. External applications or utilities must be used.

External Archiving Software

There is a software program available from Nexsan that stores and retrieves files directly to and from the Assureon.

Assureon Client (FSW – File System Watcher) – The Assureon Client software is an agent that runs on Windows systems to watch directories chosen by the administrator and will send new or changed files to the Assureon. Assureon Client is not supported for other operating systems but an Assureon Edge NAS controller may be used to provide mount points for access to the Assureon.

The Assureon Client software will load balance the file archiving among nodes in an Assureon cluster. There is an option to allow scheduled synchronization of files which can be used to schedule the archiving at less busy times. Leaving a shortcut in the Windows file system where an access to the file will retrieve the file from the Assureon is an option. The files archived may be left on the Windows file system, may be shortcutted, or may be deleted based on the Assureon Client control settings.



Nexsan Assureon

PERFORMANCE

As an archiving system, performance is usually measured in a different metric than a standard disk system would be. Archiving is really about messages, files, documents, and objects being placed in a storage environment under a set of controls. Consequently, the measure is usually about the number of objects archived per hour.

Nexsan provides a high performance InfiniBand connection to the Assureon as an option to improve the ingestion rate and access of files. There is no performance benchmark data currently available.



Nexsan Assureon

EVALUATOR GROUP COMMENTS

The Nexsan Assureon is an archiving system with a rich set of features that can operate using the standard network file protocols CIFS and NFS either directly in the case of the NXR model or through usage of the Nexsan Assureon Edge NAS system with the Assureon Client. There are several models that differ in capacity, features capability, and scaling. The CAS definition is an internal function of how data is represented for storage within the Assureon and not visible to the archiving application or user. Highlighting CAS is more of a marketing explanation of the internal techniques used and could be somewhat misleading.

Positives:

The Assureon system uses the Windows Server 2008 in a locked-down mode as a foundation for the custom software for an archiving system. This provides many advantages which were noted earlier. The included features are extensive and should meet almost any regulatory or business governance requirement. The system has been available for a number of years and should have a history regarding the maturity and reliability of the system.

The Assureon system has most of the capabilities needed in an archiving solution. There has been a great deal of progress made with the Assureon in positioning the product and establishing the market and channel sales. Most of this progress has been in the last quarter of 2010 and should provide a foundation for ongoing sales.

Potential Concerns:

The pricing for the Assureon with extra servers for different capabilities may define the market segment usage. This may limit some down-market opportunity with some customers valuing the archiving function lower than the premium would command.

For UNIX/Linux applications, the requirement to use the Nexsan Assureon Edge as a gateway to the Assureon for some models may have some very good operational usages as a staging or cache for archive data but it is initially confusing and adds some extra expense and operation overhead (management, protection, etc.) than if the Assureon could directly handle the functions as it does with the Assureon Client on Windows servers.

Having a fixed capacity with some models also may not be the best alternative for some customers. Many times customers want to start with one capacity and then add to it as necessary. If this is only accomplished with a clustered model or by purchasing additional complete systems, it may not be optimal for those customers.

Copyright 2011 Evaluator Group, Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written consent of Evaluator Group Inc. The information contained in this document is subject to change without notice. Evaluator Group assumes no responsibility for errors or omissions. Evaluator Group makes no expressed or implied warranties in this document relating to the use or operation of the products described herein. In no event shall Evaluator



Nexsan Assureon

Group be liable for any indirect, special, inconsequential or incidental damages arising out of or associated with any aspect of this publication, even if advised of the possibility of such damages. The Evaluator Series is a trademark of Evaluator Group, Inc. All other trademarks are the property of their respective companies.