NEXSAN

THE IMPORTANCE OF A SOUND DISASTER RECOVERY STRATEGY

There are a myriad of ways for organizations to lose or compromise critical data: natural disasters, fire, malicious attacks in the form of malware, ransomware or spyware, theft, hardware failure, and so on. On top of having to worry about all of the above, there's the human element to consider. Yes, everyone who uses a computer in your organization has the potential to damage, or worse, permanently delete important files.

Suffice it to say, it's imperative for an organization to maintain copies of critical content—not only for disaster recovery, but also for regulatory compliance. This is where the importance of having a sound long-term and secure disaster recovery strategy comes into play.

So, what is the best method for storing and backing-up data for disaster recovery?

Many IT professionals are turning to the cloud; but is cloud truly the be-all and end-all? Can we say with conviction that data in the cloud is secure from malicious attacks and other threats? Several recent data breaches—including one where hundreds of thousands of cloud-based voter records were left exposed by a Virginia-based robot-calling firm should have any IT professional concerned. (https://www.engadget.com/2018/07/18/robocall-exposes-voter-records/)

When it comes to cloud, there are too many unknowns: What are the vulnerabilities of the systems where an organization's critical data is backed-up? Who's responsible for patching and updating those systems, and at what frequency?

And, finally, there's the cost to consider. Not all organizations can afford to lease cloud storage for backup data that they're likely to access on a very infrequent basis.

Let's face it, despite all the cautionary tales, cloud-based storage is here to say, and some would argue that few technologies can compete with the convenience of storing and accessing data in the cloud. It's that convenience factor that appeals to many IT professionals. Unfortunately, those are the very same conveniences that can give an attacker the ability to gain unauthorized access to an organization's critical data.

So, what's an IT professional to do?

Consider a secure data archival solution as part of an organization's disaster recovery solution. A solid data archival solution can provide several benefits:

- Ensures regulatory compliance for data retention, data immutability and audit trails
- Makes archived content widely available and easy to retrieve by authorized users
- Provides policies and rules to protect from accidental deletion of critical files
- Reduces backup windows: With a copy of files in an archive, IT professionals can control backup times as there is no need to backup historical data
- Frees up Tier 1 storage, reduces media backup costs and improves RPOs and RTOs
- Allows for fast recovery of data in the event of a disaster

Nexsan 325 E. Hillcrest Drive Suite 150, Thousand Oaks CA 91360 | 1.408.724.9809

ASSUREON & UNITY ASSUREON ARCHIVE

Secure Data Capture	Assureon and Unity Active Archive (UAA) archive data directly from any local/CIFS/NFS path, and forms each file's unique fingerprint upon creation: • MD-5/SHA1 hash stays with the file throughout its life-cycle • The system validates integrity during ingestion, replication, and continuously during each file's life-cycle
Indexing	Content in Assureon and UAA is searchable by metadata (filename, directory, date modified, file size, and so on).
Information Retention	Assureon and UAA allow you to create long-term retention rules and associate them with files and folders.
Information Preservation	• Active-Active Read Failover • Native File Deduplication • Standard Assureon and UAA Replication • Read access is tracked to see who accessed the data • Data can be encrypted at rest
Information Destruction	Assureon and UAA scrub all copies of the file it has access to and then deletes the file along with its encryption key. When the encryption key is deleted, every copy of the file is effectively destroyed.
Data Recovery and Protection	• The Assureon client has the ability to replace files with stubs (shortcuts). This facilitates fast recovery time in the event of a disaster. If an Assureon Client server goes down; you need only bring up another machine, install the Assureon Client on it and the stubs can be quickly restored. • Assureon and UAA always has two copies of all data. An integrity audit regularly scans each file in the archive by comparing the file against its original fingerprint, and self-heals itself in the archive. The two copies can be at the same location or at different sites.
System Maintenance	• Access Audit Trail • Encryption of Files at Rest • Virtualized Multi-Tenancy • System state shows health of system • Email alerts when disk space is low or queues are high, etc.
Data Integrity	• Original File and Metadata Preservation • Ongoing Integrity Checking • Comprehensive Self-healing • Encryption
Date and Time Stamps	All meta data is time-stamped using secure certificates, and Assureon and UAA use a reliable time-source to ensure the time is accurate and prevent tampering.
Version Control	Assureon and UAA include built-in file versioning

ABOUT NEXSAN

Nexsan® is a global enterprise storage leader, enabling customers to securely store, protect and manage critical business data. Established in 1999, Nexsan has built a strong reputation for delivering highly reliable and cost-effective storage while remaining agile to deliver purpose built storage. Its unique and patented technology addresses evolving, complex enterprise requirements with a comprehensive portfolio of unified storage, block storage, and secure archiving. Nexsan is transforming the storage industry by turning data into a business advantage with unmatched security and compliance standards. Ideal for a variety of use cases including Government, Healthcare, Education, Life Sciences, and Media & Entertainment. Nexsan is part of the StorCentric family of brands along with Drobo – and operates as a separate division to securely protect business information.

Nexsan 325 E. Hillcrest Drive Suite 150, Thousand Oaks CA 91360 | 1.408.724.9809