# DATA AUTHENTICATION
# AND INTEGRITY
## AN ASSUREON BRIEF

How can you be sure that your archived files are in good shape—readable, accessible and not damaged? How can you truly know that no files have gone missing— deleted by accident or malicious attack?

Assureon has patent-pending technology that protects and assures the integrity of information assets that it has archived. This unique technology verifies that all files and file metadata are present and have not been tampered with or corrupted.

Assureon ensures confidence in the privacy* and integrity of your information, and in the confidence that 3rd parties, such as courts and regulatory agencies, will have that the information you provide them with is genuine and complete.

Assureon is a tamper-resistant system, purpose-built with multiple layers of safeguards to prevent, even with administrator-level access to the system and detailed understanding of its technology, any attempt at file deletion or modification. In the unlikely event that an information asset archived on Assureon ever becomes corrupted, the system, when using a redundant configuration, will automatically and transparently replace the asset from one of the redundant copies.

## Some of the technical processes used to accomplish this include:

- **Immutability**— when an asset is placed into management, a secure digital fingerprint (called a Unique File Identifier or uFID) consisting of a 128-bit MD5 hash, a 160-bit SHA-1 hash, and the file length is created. By utilizing this advanced dual-hashing process, Assureon guarantees that a file cannot be deliberately or even accidentally modified in such a way that the fingerprint remained unchanged.

- **Serialization**— each new asset is given a globally-unique sequential serial number. By serializing the assets under management, Assureon delivers straightforward validation and retrieval of assets. This is a patent-pending feature available only on Assureon.

## Key features

- Automatically checks integrity of archived files
- Immutability—archived files cannot be changed
- Self healing—ensures that all files are healthy and retrievable
- Fast access to archived files and metadata
- Non-erasable, non-rewritable functionality

- The fingerprint and various other data about a file such as its name, date of creation, retention policy, asset serial number, encryption key serial number, and source path, are combined into a metadata record which is digitally signed and bound to the asset.
- During every retrieval of a file, and periodically as a background task, the contents of the metadata are checked for internal consistency and the stored fingerprint is compared to the actual fingerprint re-calculated on the asset. Discrepancies are logged and any defective asset is replaced with one of the redundant copies kept on the Assureon system. This is done automatically and is transparent to the user unless there is an error with a file. If Assureon is configured in redundant mode it will self-heal the file or replace the deleted file.
- Assureon provides WORM emulation in that assets may not be modified ever, and may not be deleted until the document expiry date has been reached and then only if no deletion inhibit flags have been set (e.g. in response to an e-discovery motion).
- File deletion at the end of the retention period requires confirmation by a human operator.
- Since each file has a unique encryption key, at the end of the retention period all copies of the key are destroyed, effectively deleting all copies of the file including copies held on removable media. This is called "assured individual key destruction" and, in contrast to some competitors who claim similar features, Assureon enables selective destruction to the individual file level rather than just whole tapes or directories.
- Assureon produces frequent audit reports to provide confidence that the security and integrity features are working properly for all assets. Regular electronic inventory checks are performed checking the sequential serial number list of all assets.

\* When used with Assureon's secure encryption feature. For more details on this technology please read the Assureon Brief on Data Privacy and Theft Prevention

# NEXSAN

## ABOUT NEXSAN

Nexsan® is a leading provider of innovative data storage systems with over 10,000 customers worldwide. Nexsan's pioneering hybrid storage systems combine solid-state technologies, spinning disk storage and advanced software to deliver radical new levels of performance and capacity at lower cost. The company's advanced technologies enable organizations to optimize traditional, virtual and cloud computing environments for increased productivity and business agility. With more than 28,000 systems deployed since 1999, the company delivers its data storage systems through a worldwide network of solution providers, VARs and system integrators. Nexsan is based in Thousand Oaks, Calif. For more information, visit **www.nexsan.com.**