NEXSAN

SOLUTION BRIEF
SILENT DATA CORRUPTION IS REAL... HERE'S HOW TO BEAT IT

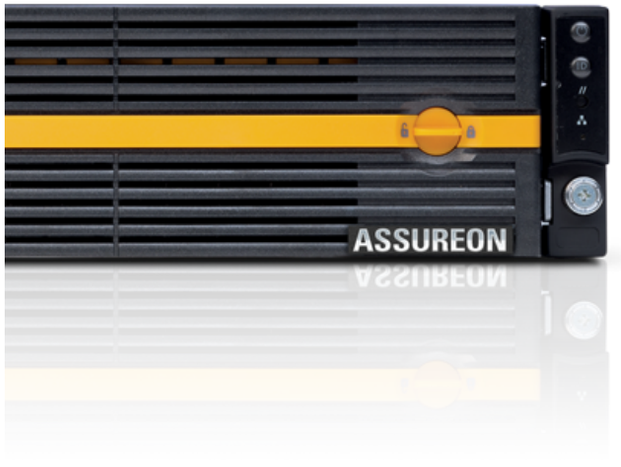
Silent data corruption is real and must be taken seriously. This threat is not an abstract "theoretical possibility," rather a real-world risk that's been reported by hardcore researchers for several years. As early as 2007, the world-renowned CERN research organization tested 3,000 servers attached to RAID subsystems; in three weeks it found 500 instances of corrupted files in 17 percent of the RAID arrays. In short, the equivalent of **one in every 1,500 files had become corrupt.**

That's bad, but even worse is how easily silent data corruption can take place without notifications. Oracle stated in February 2013, "[It] can happen without warning and can be defined as the non-malicious loss of data resulting from component failure or inadvertent administrative action. Silent data corruption occurs when invalid data is read or written rather than resulting in a failed I/O operation. This type of corruption is by the far the most cataclysmic, and **there are no effective ways to detect it without end-to-end integrity checking."**

OK, let's back up to that disheartening last sentence. With active files (i.e., ones that are constantly being accessed and opened), any data corruption or missing files will quickly be noticed. But it's a completely different scenario with your archive files, which are rarely opened — usually only when they are critically needed. It could be months or even years until you discover one of your files is damaged...or gone.

Corrupted or missing files are obviously a huge problem for healthcare, financial services and governmental institutions because they're subject to rigorous regulatory requirements. But this problem really threatens any organization that archives high-value data. A great deal of companies are affected, and odds are you're at risk, too.

What's the solution? As noted, end-to-end integrity checking is the only way that silent data corruption can be detected and corrected. Simply put, **any archive solution that lacks this integrity checking cannot credibly claim to offer secure archiving...period.**



[1] *Data integrity, Bernd Panzer-Steindel, CERN/IT Draft 1.3 8., April 2007*

[2] *How to Prevent Silent Data Corruption, Martin Petersen and Sonny Singh, published February 2013, http://www.oracle.com/technetwork/articles/servers-storage-admin/silent-data-corruption-1911480.html*

HOW NEXSAN ASSUREON COMBATS SILENT DATA CORRUPTION

Conventional archive solutions can't monitor the availability and health of every file, and manually verifying the existence and integrity of those files (by opening millions, perhaps billions of them) would be a nightmare. If you want true end-to-end integrity checking, you must have a secure archive solution that's been specifically designed to maximize data security, integrity and privacy from the moment a file is ingested into the archive. That's exactly what Nexsan Assureon™ does.

Assureon's ingestion process begins with duplicating each of your files, stored either in a separate RAID disk set within your local Assureon system or on another Assureon you've installed in a remote location, such as your main office or in the cloud. Maintaining a second, redundant copy of every original file is key because it enables Assureon to perform crucial comparative analyses of your files using these two powerful data protection technologies:

- File serialization
- File fingerprinting

Figure 1: *Assureon's unique file serial numbers enable easy identification of missing files.*

FILE SERIALIZATION

Every file ingested into Assureon has a unique serial number assigned to it (used for both copies of a file, the original and its redundant copy). This file serialization enables Assureon to periodically verify the existence and location of every file in the archive, both at the archive's primary site and at its secondary site. If a missing file is detected, Assureon can notify your administrator and automatically replace it using its serialized redundant copy *(see Figure 1)*.

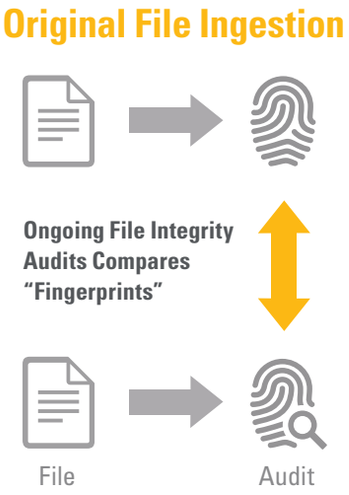


Figure 2: *Unique fingerprint enables recurring checks for corrupted files.*

FILE FINGERPRINTING

To guarantee file-level integrity within the archive, Assureon generates a unique gold-standard "fingerprint" of each file when it is ingested and when it is copied. Subsequent copies of the original file (for example, stored in a remote location) can be validated as a correct copy of the original file after the copy's fingerprint is compared to the original's fingerprint. Assureon performs this file fingerprinting by combining two hashing algorithms (MD5 and SHA1) on the same file.

These fingerprints enable Assureon to periodically audit the integrity of each file against its original fingerprint, in order to confirm the data has not been changed (due to silent data corruption, disk error, virus, tampering or replication error). Should this process reveal that one of your archived files has been altered, the audit reports the corruption and Assureon automatically replaces the corrupted file with its undamaged copy *(see Figure 2)*.

Nexsan 900 E Hamilton Ave Suite 230, Campbell CA 95008 | 1.408.724.9809

> This type of corruption is by the far the most cataclysmic, and there are no effective ways to detect it without end-to-end integrity checking."
>
> **ORACLE**

ASSUREON: MULTI-PRONGED DEFENSE OF ARCHIVE DATA

1. **File Integrity:** Each time a file is saved, a unique fingerprint is generated using both an MD5 and SHA1 hash of its contents and metadata to ensure history and contents cannot be altered after the fact. Every 90 days the integrity of every file is automatically audited against the original fingerprint.
2. **Data Availability:** Each file is assigned a unique serial number which is used to ensure no files are missing or inappropriately added. Every 90 days every file is automatically checked to make sure it is still in the archive.
3. **File Redundancy:** Each file and its fingerprint are stored twice by Assureon; the second copy is stored in a separate RAID disk set within the same Assureon unit or on a remote Assureon.

DON'T BE FOOLED BY OTHER "SECURE" ARCHIVE SOLUTIONS

Unlike other solutions claiming to be secure archives, Assureon proactively ensures your data is always there by *automatically performing a background fingerprint and serialization file integrity audit—no user intervention required.* By contrast, some secure archive solution vendors also utilize fingerprints to monitor file integrity, but they *only check the fingerprint against its file when you access the file.*

That's a big problem, because you'll find out you've been hit by data corruption only when you try to open the file—and by then all hope of replacing that damaged data may be lost. The only way you can combat this is to purchase expensive backup/dedupe appliances and tape backup. So in the end, your investment in these "secure" archive solutions doesn't really guarantee you anything except the need for a massive increase in your IT spending.

HOPE IS NOT A STRATEGY

Silent data corruption is an unfortunate reality in the IT landscape; its occurrence is not a question of "if" but "when." Just hoping this phenomenon won't eventually strike conventional archive solutions is hardly an effective strategy. **The answer is to proactively protect your archived files by deploying a Nexsan Assureon secure archive solution, purpose-built to maximize your data's integrity and security.**

ABOUT NEXSAN

Nexsan™ is leading the way in redefining unified storage. With a solid reputation for delivering reliability, cost-effectiveness, and unrivaled customer service, Nexsan has always developed world-class storage technologies that are focused on the critical needs of our customers. Our renowned E-series is the storage backbone of many data centers around the world due to its high performance, reliable, high density storage. Headquartered in Campbell, California, Nexsan is a wholly owned company of Imation Corp. (NYSE:IMN). For more information, please visit: www.nexsan.com.

Nexsan 900 E Hamilton Ave Suite 230, Campbell CA 95008 | 1.408.724.9809