SISCIN

SISCIN TripleLock Archives

Unalterable Storage for Compliance Retention

"€3.3million is the average cost of a data breach worldwide and 52% of data breaches are caused by malicious attacks."

- IBM

SISCIN TRIPLELOCK

"A Patient has died after a Ransomware Attack Hits a German Hospital",
according to MIT Technology Review. The outage resulted in a significant delay in treatment. German authorities are investigating the perpetrators on suspicion of negligent manslaughter.

RANSOMWARE HAS EMERGED as one of the top threats facing organisations, large or small, with researchers reporting more than a fourfold increase in detections last year. Organisations like yours, accumulate a lot of data, you need to store that data in an unalterable way to protect it from Ransomware.

Waterford Technologies' has you covered with SISCIN TripleLock Archives. This security addition to SISCIN file archiving offers immutable write once read many, compliance storage that is both secure and easy to use at no additional cost.

THE SISCIN TRIPLELOCKS ARE

Protected by your Credentials

Protected by SISCIN AES Encryption

Write Once Read Many (WORM)

SISCIN TripleLock archives allow organizations to quickly implement WORM technology that makes immutable "locked" copies of their data within the cloud, thereby providing comprehensive ransomware protection. When you create a TripleLock archive (or convert an existing archive to TripleLock (LLL)) you are making the objects within that archive read-only for a defined period. This can be from 24 hours to many years. This gives the best assurance possible that your data is safe. Each object within a TripleLock archive has its own timer. For instance, if you create a 1-year TripleLock archive any file added to that archive is secure for 1 year from the time it was archived.

Powerful SISCIN TripleLock Archives for Ransomware Defence and Recovery

BENEFITS/FEATURES

Ransomware Defense and Recovery

- Archive files directly to Immutable (WORM) Cloud Storage.

- Quick recovery from successful premise attack - Restore original file back to its original or alternate location.

- No need to worry about backup re-cycling or expiration, protection \ cover can persist for years if required.

Secure Document Retention

- Time-based retention - Data cannot be deleted or modified by user or system, including account administrative privileges.

- Prevents container deletion.

- Prevents storage account deletion.

Ensures Regulatory Compliance

- Immutable storage helps organisations address SEC 17a-4(f), CFTC 1.31(d), FINRA, and other regulations.

- Satisfy auditors with bullet-proof immutability of your file data.

Legal Hold

- Enables organisations to store sensitive information that is critical to litigation or business use in a tamper-proof state for the desired duration until the hold is removed.

Will you be the next ransomware victim?

Unlike backup and legacy WORM archives, Waterford Technologies is an affordable file archiving solution that includes TripleLock at no additional cost as well as built-in content indexing and discovery search. WORM eliminates the fear of ransomware attacks by making data unchangeable until a specific time has passed, preventing malware from encrypting data and locking users out. Because the data cannot be altered, it cannot be encrypted by ransomware.

Revolutionise your compliance archiving strategy, protect your organisation from ransomware and meet key regulatory requirement all in one package. Contact us today and get protected.

STL_DS_EMEA_10_20

WATERFORD TECHNOLOGIES

EMEA: +353 (0) 51 334 967 | UK: 0845 378 0935 | USA: +1 (949) 428 9300

sales@waterfordtechnologies.com | www.waterfordtechnologies.com