SISCIN

Performance, scalability and flexibility with peace of mind

DATASHEET

SPLIT VOLUMES

When you archive to the SISCIN platform you send data to SISCIN Archive Volumes. These volumes reside in your Azure or AWS storage accounts and you always have full control and management of them.

For your peace of mind, SISCIN offers a number of archive volume types, just choose the most suitable depending on your businesses unique requirements and security goals.

1. SINGLE VOLUME

Each file you archive is placed in a single storage endpoint, always compressed, deduped and encrypted.

2. DOUBLE VOLUME

Each file you archive is copied to two storage endpoints. These can be with different storage providers, so for instance you can have one copy with Azure and another with AWS. Again, these are individually compressed, deduped and encrypted to each storage provider. At retrieval time, if one provider is unavailable SISCIN will automatically retrieve it from the other.

SISCIN Security

SISCIN is designed to be highly scalable and highly available. Utilizing the Microsoft Azure platform to ensure we provide the maximum security, resilience and uptime at all times.

FEATURES

ENCRYPTION

When you archive your files to the SISCIN platform your file data is compressed and encrypted before it leaves your premises. This is a full AES based encryption and uses keys that are unique to your account. Additionally, all transfers to or from the cloud platform are also SSL protected.

KEYSTORE

Your individual KeyStore is a critical part of the SISCIN Cloud Platform. For your organisations protection each object that you archive is encrypted with a unique Key, these keys are securely stored in your KeyStore. You always control the KeyStore, it is always unique to your organization, lives in your Microsoft storage account and is NEVER shared with any other platform users.

WATERFORD TECHNOLOGIES
Email & File Compliance Solutions

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

sales@waterfordtechnologies.com | www.waterfordtechnologies.com

SPLIT VOLUMES

3. SPLIT VOLUME

When higher levels of security are required SISCIN has the ability to split each individual byte of your file across two providers. NO RECOVERABLE DATA is available from either provider, at retrieval time the SISCIN platform will reassemble your data for you prior to delivering it back to your users. This is all done in real-time, is transparent to users and is in addition to our normal compression, de-duplication and encryption of your data.

4. SPLIT-R VOLUME

The SISCIN Split-R offers our highest level of security and resilience. Like the Split volume we store each individual byte of information across two different locations, ensuring no single location has any recoverable data. In addition to the Split volumes security Split-R add a third location for resilience. Should any location be unavailable for any reason the SISCIN platform will reassemble your data from the information stored at the two other locations. This recovery is automatic, is done in real-time and is transparent to your users. This extra security and resilience come in addition to SISCIN's standard compression, deduplication and encryption

OUTGOING PORTS

Communication between SISCIN Server Agents and SISCIN in the cloud runs across the internet. All information gathered by SISCIN Server Agents is encrypted and compressed on your File Server before it is sent to SISCIN in the Cloud. To do this securely specific TCP Windows Ports need to be open OUTBOUND to allow the SISCIN Server Agents to communicate with SISCIN. The following ports must be open OUTBOUND from the SISCIN Server Agents in Windows Firewall, Routers and any other device that controls access to the internet. Contact your Network Administrator if you are unsure how to open these ports in your organization. · Ports 80 and 443 must be unblocked OUTBOUND to *.blob.core.windows.net · Ports 5671, 5672, 9350 – 9354 must be unblocked OUTBOUND to *.servicebus.windows.net. We NEVER ask you to open an inbound port for the SISCIN Cloud platform.

USER ACCESS

ADMIN

Any member with administration rights or role has the ability to carry out almost all SISCIN functions. The only restrictions is that they can't do a content search nor can they download any data directly through the browser. The Admin user can still search, but only by file name, watchpoint, folder etc

SEARCH USER ROLE

Users can be given the 'Search User' role for DPO's, compliance managers or data controllers. With this role, the user will be allowed to search within file content of files. This user will not be able to carry out ANY agent management, they will therefore not be able to create watchpoints, setup or initiate policies etc.