SYNKZONE

by safespring

A truly secure file storage and collaboration service built for businesses and professional organizations

Synkzone combines the flexibility, accessibility and ease of use of cloud storage with the control of the traditional file server. Synkzone is a truly secure service designed from the ground up to meet enterprise security requirements.

SECURE SHARING Information is organized into zones and it is only the members of a zone who are allowed to access and collaborate. Sharing outside the zone is possible of individual files by using secure download links.

SECURE STORAGE
All data is encrypted at rest, safely stored in Safespring data centre.

COLLABORATION IN ZONES
A flexible, and business friendly way to organize data.

BUILT-IN RANSOMWARE PROTECTION
Synkzone automatically detects infected files and isolates infected nodes. After the ransomware has been removed the client restores all files.

TRULY SECURE

- Strong multi-layer encryption
- End-to-end security
- Zero knowledge

Security and control

SYNKZONE by safespring

Synkzone provides full control over your organization's information and does so using the best security architecture available. The service is built around the 'zero knowledge principle' meaning that neither Synkzone as a service provider nor any other unauthorized party can access the information stored in the service. There are simply no backdoors.

SECURE SHARING INTERFACE The Synkzone Secure Sharing Interface (Synkzone SSI) provides an API (Application Programming Interface) towards the service. Using the API it is possible to integrate the Synkzone service with other systems, new or legacy. This approach opens up for many new possibilities.

SECURE STORAGE By using the Synkzone storage an increase in control, reliability and security can be achieved. Sensitive information no longer needs to be stored in the original system but may be stored securely in the Synkzone service instead.

SECURE SHARING Relying on Synkzones mechanism for sharing and collaboration makes it is easy to create solutions where information is shared in a secure way. In Synkzone information is organized into zones and it is only the members of a zone who are allowed to access and collaborate. Each member in a zone has a unique access level ranging from read only to full zone management rights. Sharing outside the zone is possible of individual files by using secure download links.

REST API The Synkzone SSI offers an easy to use REST API. The API enables secure connections between external services and Synkzone. The connections are based on the OAuth2 protocol specification.

The API can be used in a number of different scenarios, ranging from the creation of new services and features that extend the basic Synkzone functionality, quick increase of the security and usability of legacy systems or to simplify and off–load the security design of new systems.

USAGE EXAMPLE One usage example is to have all the file handling done in Synkzone. This involves all aspects of the life cycle of a file from creation, transfer, storing, distribution and secure access. By using Synkzone it is possible for the external system to handle files by reference only. The references are not sensitive and can be both stored and distributed. References are used to access files but it is only possible by users who have been given the authority to do so.

TRULY SECURE Using Synkzone you, and only you, decide where your information is being stored and who has access to it. Synkzone provides a multilayered security approach with several strong security features:

STRONG MULTI–LAYER ENCRYPTION Communication in Synkzone is done using a multi–layered security approach. All messages are encrypted and signed between the communicating nodes (end–to–end). Only trusted nodes are allowed to communicate with each other. Sensitive information is encrypted by the application layer before they are inserted into the messages. Lastly links used for point–to–point communication such as TCP use TLS 1.2 for security.

END–TO–END SECURITY The message system within Synkzone uses end–to–end security so regardless of what links are used the messages are secured end–to–end. The same applies to all file handling. Files are encrypted in the clients when they are added to the system and are transferred and stored in their encrypted format (called Storage Files). Only an authorized user on a client can decrypt a Storage File. During all other life cycle phases of the file (transportation, caching and storage) the storage file exists in its encrypted format and the systems involved do not have access to the encryption keys.

ZERO KNOWLEDGE In Synkzone encryption is done using encryption keys not available to anyone else but those who are authorized by the customer. This means that neither Synkzone as a service provider, nor anyone else, has access to the customers information or encryption keys. Zero knowledge provides protection against unauthorized parties that have gained access to the infrastructure regardless of if they are network managers, hackers or other. There are simply no backdoors!

COLLABORATION IN ZONES In Synkzone information is divided into zones. Zones are a flexible and business friendly way to organize an organizations data. A zone can represent, for example, a department, a project, a management group etc. In a zone information is shared between its members. Each member of a zone has personal access rights, easily defined by the administrator of the zone. Only zone members have access to the information in the zone (files, chat, log etc.).

SAFE ZONES This is a special zone where information is not allowed in clear text on a user client other than temporary. This zone type provides additional security for sensitive files.

RANSOMWARE PROTECTION Synkzone has a built in protection system against ransomware. Synkzone automatically detects infected files and isolates infected nodes. After the ransomware has been removed the client restores all files.

CONTACT US
info@safespring.com
www.safespring.com