File StoredSafe

Most organizations have highly critical and confidential information such as trade secrets, proposals, financial data, mergers & acquisitions, etc. The loss of this data could potentially jeopardize the organization, and cause a major impact to the organizations reputation resulting in significant financial damages. Even though strong security controls may be in place, the risk for loss of this data would be such a significant event that further mitigation should be considered. This type of event could also be classified as a black swan event*.

*Black swan event is a metaphor that describes an event that comes as a surprise, has a major effect, and is often inappropriately rationalized after the fact with the benefit of hindsight.

As the threat environment (insider trading, hackers, industrial espionage, disgruntled employees, outsourcing) has changed, more organizations are realizing the need to further define additional security requirements to protect highly confidential information. Due to the significant risk reduction, low cost and business needs the time has now come to implement File StoredSafe to improve the management of the organization's highly confidential information.

File StoredSafe is used d to store and share any type of file or document in a secure manner. It further enables an organization to assure and prove that the information is restricted, only accessed by authorized individuals and provides an audit log of who has seen what information and when.

You are also able to share this information in a fully controlled manner to external individuals. Not even your File StoredSafe system administrators will be able to read your encrypted information. The information owner remains in control. This product is especially beneficial for protecting highly confidential information against the risk of unauthorized or unintentional access, hacking attacks, disgruntled employees and vendors. In addition, this is also a valuable solution when there is a need to store highly sensitive information at other physical locations such as a hot site for disaster recovery, emergency management, outsourcing, etc.

File StoredSafe is used by our customers to store highly confidential data such as:

- Intellectual Property (patents, code, recipes, product development etc.)
- Board Reporting
- Financial Reporting (before publishing date)
- Due Diligence Information
- Critical IT-Infrastructure Documentation
- Merger and Acquisition Information
- Internal/External Investigations
- Critical Backups (HSM's, encryption keys etc.)

Our solution easily integrates with your current IT infrastructure without any major redesigns.

StoredSafe is a premium security appliance company utilized by organizations who have strong business security requirements related to critical data that needs to be shared with internal/external parties over time and in an auditable way.

STORED SAFE

Secured Storage and Sharing of Highly Confidential Information

STORED🔒SAFE

Technical Specifications

StoredSafe Secure Platform
All of our products utilize the StoredSafe Secure Platform. Our unique architecture puts the information owner in control of the information on a scalable platform and enables an organization to choose between our products, based on their needs as well as adding functionality over time.

StoredSafe Audit Engine
All events in StoredSafe Secure Platform are logged and traceable in our easy to use audit engine.

2-factor Tokens
StoredSafe is designed to store your most confidential information. Therefore, two factor authentication is required and included as part of the StoredSafe Secure Platform. Our preferred, recommended solution is Yubico's YubiKeys as a hardware token in addition to a strong passphrase.

Hardware Security Module (HSM)
To further improve security, YubiHSM is incorporated in the platform to protect cryptographic keys for all YubiKey hardware tokens. This provides a self-sufficient YubiKey validation server and enables our customers to be independent of Internet connectivity.

StoredSafe Overview
Strong Encryption
To assure confidentiality over time all StoredSafe products can easily change encryption algorithms and modes (OFB, GCM, etc.) as needed without putting current data at risk.

Data at Rest
StoredSafe utilizes 4096 bit RSA Keys for asymmetric encryption and AES-128 in OFB mode for symmetric operations.

Data in Transit
StoredSafe uses TLS for protection of data in transit.

Role Based Access Control System
StoredSafe utilizes a Role Based Access Control System (RBAC) to supply a fine grained control of user capabilities and vault permissions.

Defining requirements, procure and implement a secure file storage solution could be a challenging task. Below are some of the key factors an organization should consider for a secure file storage solution

Desired Outcome	Factors to Consider	File StoredSafe	
Owner of information should be in control of the information.	Can only the information owner grant access to the information?	File StoredSafe has no master key. Not even a system administrator can access information, unless the information owner has provided access.	✔
Access on a business need to know basis.	Does the solution support relevant business roles and responsibilities?	File StoredSafe has a comprehensive and flexible RBAC system which is easy to administer.	✔
Full traceability.	Will the solution provide a full audit trail on all important events?	StoredSafe Audit Engine provides a full audit trail.	✔
Cost efficient setup for external information sharing	Does the solution facilitate information sharing with outside organizations?	Sharing information with one or more outside organizations with File StoredSafe is easy and cost efficient.	✔
Cost efficiency	Total Cost of Ownership (TCO)	StoredSafe has a low TCO, a low cost for implementation and low annual operational cost.	✔
Scalability	Growth in number of users	StoredSafe can grow to thousands of users and additional StoredSafe functionality by adding modules as needed.	✔