



Predict | Protect | Prevent



ARCON | My Vault

Overview

- Where do organizations store this critical information?
- Who has access to this critical information?
- With whom are employees sharing the information?
- Do your organization identify unauthorized users who try to access any business-critical information?

If there is uncertainty with any of the above questions, there is a serious need to ponder over the crux of secure storage of enterprise data. Generation and accumulation of enterprise data is a continuous process, and the volume increases simultaneously with the organization's growth. It requires data security, data integrity and data privacy. Even if the organization ensures robust access control practices to restrict unauthorized access, data security could be compromised if there is no storage mechanism or loopholes in the storage mechanism. It requires the Zero Trust model to secure critical business data assets.

Now the question is - is this impenetrable security possible only through IAM (Identity Access Management) practices or by deploying enterprise-class PAM (Privileged Access Management) solution?

ARCON | My Vault complements PAM or IAM solution which is an advanced and secure centralized repository to vault, share, and access critical data assets. It dramatically improves the Zero Trust posture by providing adequate controls over storing and sharing critical data assets.

Moreover, the files where this information is stored remain encrypted and can be deleted after a preset time. ARCON | My Vault also controls the end-users' activities at a granular level based on the pre-configured permissions. It provides administrative users managing servers the ability to transfer files from one machine to another without going through the interactive access in Privileged Access Management.

The advantage of ARCON | My Vault is that it can be used as a discrete solution (with or without PAM). It is based on a microservices framework and is built for the cloud. However, the solution can also be installed on-premises for PAM customers. In addition, the discrete solution has advanced features like onboarding user groups, tagging businesses, workflow, just-in-time access to secrets, keys, certificates, files, etc. Furthermore, one can provide role-based access for sharing, downloading, viewing, or transferring files and secrets. My Vault also provides simple centralized storage for exceptionally large files.

How does ARCON | My Vault work?

ARCON | My Vault solution is secured with multiple layers of security which include firewall, authentication, authorization, access control, and encryption. These layers make the solution secure for usage by any small or large organization. It can be deployed within a brief period and can be accessed through the Web interface. It is primarily built for the IaaS infrastructure, but it can also be installed on-prem in the Privileged Access Management (PAM) environments.

Users can perform operations such as uploading, downloading, viewing, and deletion of files from the vault just as one does on a regular drive. Files are stored on the centralized server, configured by the Administrator, and all Secrets added or uploaded are stored in an encrypted format in the database. Hence, users can share documents, spreadsheets, images, certificates, SSH Keys, video, and/or audio files with others directly or to the public via a link without sending them through email or printing it out.

ARCON | My Vault architecture is quite simple and seamlessly integrates with the complex infrastructure of an enterprise. It consists of three important components:

- 1. Secured Vault:** It stores data and protects it through authentication and authorization.
- 2. Secured Gateway Server:** It uses a unique technology of secured ports to channelize all the traffic directly from a user machine to the target devices.
- 3. Batch Processes:** It helps My Vault to run on a predefined schedule and execute the tasks in the background.

ARCON | My Vault

Key Features

Here are the exclusive features of ARCON | My Vault that help organizations in distributed IT environments manage, store and access enterprise data safely in various file formats such as .xls, .doc, .xml, .csv, .pdf, .ppt etc. along with folders, drives, keys, certificates, and secrets.

Unique Features



Ownership Transfer

It ensures seamless administrative experience with My Vault's unique ownership transfer capability which allows one user to transfer file rights to another user when the former leaves the organization or joins another line of business/ department.

Whitelist & Blacklist File types

The administrator can whitelist the file types that should be supported in the My Vault Application; rest of the file types are automatically blacklisted/ restricted for the My Vault users to enhance security posture.



Audit Logs

My Vault provides audit logs that show the entire user activity on a given date and time. End-user logs enhance best-practices as to data security as it enables admins to review operational activities performed on each data file or business secret by any end user.

File Request

With this feature, the users of My Vault can request to Download/Share/Transfer data files from the owner who has uploaded publicly with file request permission.

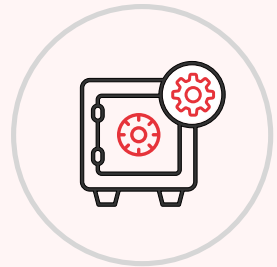


Team Management

Team Management functionality allows users to share Files/Folders/Secrets with team and users who are part of it and can view it anytime.

Dynamic Secrets Management

It helps to protect valuable data, including PINs, web applications, certificates, services, and SSH keys, involves implementing robust practices to ensure the security of sensitive information.



Vault SSO For Web Applications

Users in an organization can take Single Sign-On (SSO) of web application configured in My Vault using My Vault Plugin or My Vault Application.

Auto-Uploader

With the help of Auto-Uploader, any data file/ folder located in the client's server of different domain can be copied and shifted to My Vault to ensure safe storage of the data. It carries the default restrictions of sharing rights and limitations to ensure unauthorized access/ sharing/ download.



My Vault DRM tool

DRM (Data Risk Management) tool allows users to sync files and folders with My Vault. It protects digital content by controlling how it can be accessed, copied, and distributed. It ensures that creators and distributors maintain control over their intellectual property, preventing unauthorized use and piracy.

Cross Domain Sharing/Collaboration

My Vault allows users to share and collaborate on files and folders with users from different domains, offering granular control configured in the vault. Cross-domain users must complete two-factor authentication (2FA) before downloading any shared files or folders, ensuring enhanced security.



General Features



File & Secret Storage

ARCON | My Vault offers a centralized repository to store, access and share critical business secrets in a secure manner. The files where this information is stored remain encrypted and can be deleted easily after a preset time to avoid any unauthorized access. It also controls the end-users' activities based on the pre-configured permissions even at a granular level. It minimizes the risks of data misuse.

File Sharing and File Transfer

While sharing or transferring data files from one user to another, ARCON My Vault can customize end-user access and sharing permissions. It allows the sender to restrict the receiver from downloading the shared file as many times as possible and even apply sharing restrictions on random transfer of that data file with internal employees and people from other email domains. After the predefined period, the shared file access/ download/ transfer rights are revoked automatically.



Controlled File Types

The administrator of ARCON | My Vault can easily whitelist the file types that should be supported in the My Vault Application; rest of the file types are automatically blacklisted/ restricted for the My Vault users to ensure security.

Centralized Engine for Data Assets

With this, the IT risk management team can mitigate catastrophic risks arising from uncontrolled data spreads by implementing My Vault unified engine to manage, restrict, and control end users' access to every piece of confidential information.



Zero Trust Approach

Organizations can reduce the enterprise data attack vector as My Vault provides multifactor authentication, just-in-time privileges and role-based access control that support Zero Trust approach.

ARCON | My Vault

Benefits at a glance

Ensures secure uploading and sharing of data files and business secrets

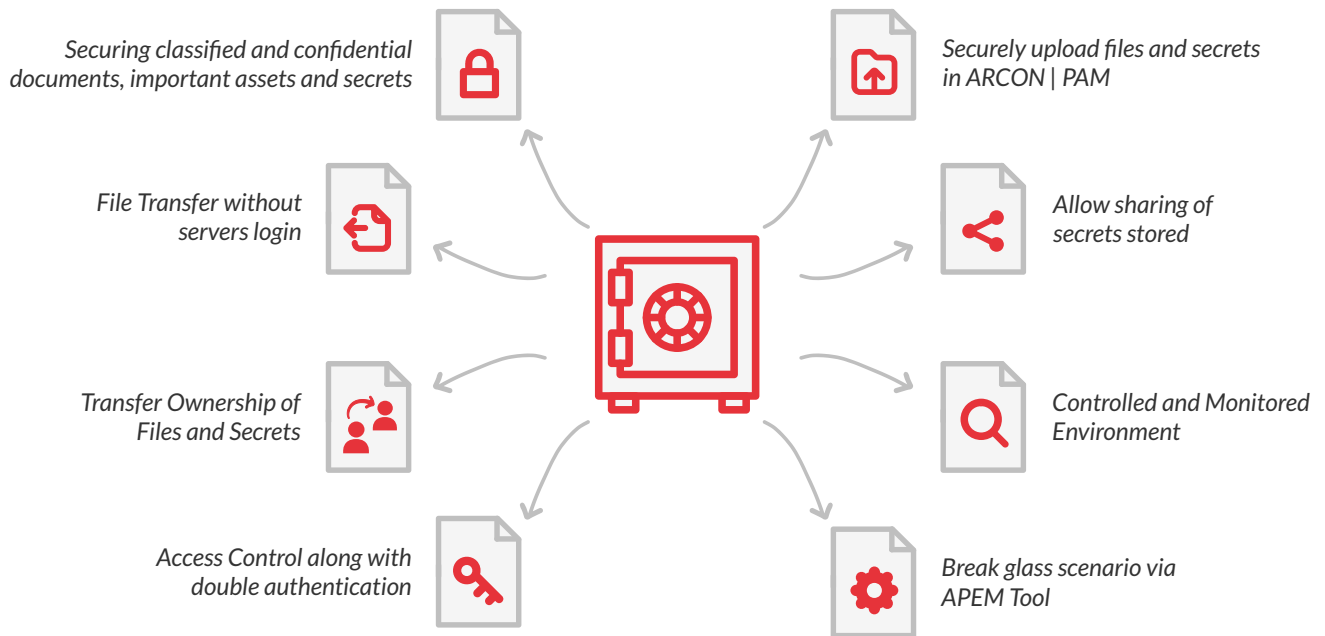
Provides end-to-end data encryption

Automates the process of deleting data files right at the designated time

Ensures data integrity and desired data confidentiality

Meets compliance with the global & regional IT standards

Product Architecture



About ARCON



ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.

All rights reserved by ARCON

This document or any part of the document may not be reproduced, distributed or published in any form without the written consent of the copyright owner under any circumstances. Any kind of infringement in the owner's exclusive rights will be considered unlawful and might be subject to penalties.