DATAVAULT - A COMPREHENSIVE SECURE FILE REPOSITORY SOLUTION

CONTEXT

Every organization has a treasure trove of sensitive data and information in the form of digital files and documents. Competitors, hackers, and others are constantly trying to exfiltrate such documents and files for various reasons. There is also a worrying trend related to data theft by insiders, either inadvertently or with malicious intent which is exceedingly difficult to handle. Currently, no comprehensive solution is available in the market to secure sensitive files and documents from different types of data theft attempts.

DATAVAULT IS OUR SOLUTION

Most Secured File Repository Solution for Organization's Sensitive Files or Documents, Built on patented SolidWall technology

DataVault is a data security appliance. It offers secure storage space to organizations for storing and managing their sensitive files and documents.

In DataVault, your files and documents are secured and protected by multiple layers of industrystandard security tools along with our proprietary and patented SolidWall Technology. SolidWalltechnology's main security feature is to remove all possibilities of data theft and data manipulation while providing modern features to help manage and access your data in a completely securedway.

The file storage space offered by DataVault is further segregated into separate storage entities called "Vaults". Each Vault is isolated and completely independent from other Vaults on the sameDataVault instance.

"Vault Owners" have exclusive rights on their assigned vaults. For illustration purposes, we can consider the example of bank lockers. Within a bank's locker room, multiple lockers are completely isolated from each other. Individual lockers are accessible only to their respective owners. Similarly, a Vault owner within the DataVault instance has an exclusive and absolute right on all data stored within their vaults.

WHY DATAVAULT?

Currently, no integrated solution is available in the market which offers comprehensive protection to sensitive information stored in the form of files and documents. Typically, security solutions focus only on one or two aspects of the entire problem. Organizations have separate solutions for Identity and Access Management (IDAM), network protection (firewalls, IDS/IPS), encryption, endpoint protection, Data Loss Prevention (DLP) based solutions, etc.

But the issue is that:

- They are not designed specifically for protecting your organization's confidential files and documents. Therefore, they lack key data security features to provide comprehensive protection for such requirements.
- When they are implemented as standalone solutions, they can be circumvented.
- Integrating such solutions which are often from multiple OEMs is expensive and sometimes not even feasible, either technically or financially.

Therefore, enterprises need a comprehensive solution to protect their confidential documents and files without spending time and money integrating complex solutions and legacy systems.

Security features of DataVault make it a perfect solution:

Designed with a security-first approach, DataVault is designed for securely storing and managing sensitive information. DataVault meets the stringent security requirements for your most important files and documents in one single appliance which in the past required multiple productimplementation and integration.

Its security features consist of:

- **Proprietary Active Exfiltration Protection Engine**
- **Proprietary Restricted Shell** to control user activity
- **Adaptive Multi-Factor Authentication**
- **Immutable Data Enclave**
- **FIPS 140-2 complaint** encryption algorithms and **Transparent Encryption** to protect data at rest and in transit
- **Granular User Behavior Monitoring**
- **Secure Viewing and Editing Features**

- **Anti-Virus Scanner**
- **Zero-trust Policy** and audit trails
- **Secure, Self-hosted, Scalable** product which can be deployed as an on-premises, standalone server as well as in a datacenter

IMPORTANT FEATURES OF DATAVAULT

- **DETAILS OF SECURITY FEATURES**
    - **Active Exfiltration Protection (AEP) Engine**: AEP engine is designed to deny all data exfiltration attempts from within the secure storage environment of DataVault, by default. AEP protects your sensitive data against attempts of exfiltration by hackers as well as from unauthorized data exfiltration from malicious insiders.
    - **Restricted Shell:** Our other proprietary solution, the Restricted Shell controls user actions within DataVault. User actions are governed by segregating users as per their access level and limiting them only to a set of pre-approved actions that a user can perform on a particular file.
    - **Ransomware Protection:** We have implemented an immutable data store for your storage needs, which assures a certain degree of data protection from ransomwareattacks on the files stored inside DataVault.
    - **Encryption at Rest and in Motion:** DataVault implements FIPS 140-2 compliant encryption algorithms to encrypt files at rest and in motion within DataVault.
    - **Transparent Encryption:** Files and documents protected by DataVault can be accessed only through its web user interface. DataVault encrypts all files if any other application or malicious code tries to access those files and documents without the protection offered by DataVault. This ensures that your sensitive information is always protected from data theft.
    - **Anti-Virus Scanner:** DataVault scans every file for malware at the time of file upload. Any malicious file is quarantined, and the main data store is protected from all known viruses and malware.
    - **Multi-Factor Authentication (MFA):** DataVault has a mandatory two-step verification process for user login right from the very first login attempt. As of now, we have integrated Google Authenticator for generating the time-based security

tokens for the second-factor verification (available on iPhone, Android, Windows Phone).

- **Adaptive Multi-Factor Authentication with User Behavior Monitoring:** DataVault takes user verification to an advanced level by verifying the identity of users even when they are in session and challenges them to verify themselves whenever:
    - an action performed by the user deviates from their past behavior
    - the user performs a critical action, which is pre-configured for re-verification
- **User Administration and Access Control:** DataVault also implements best security practices and workflows like user administration and granular level-access controls. This restricts all unwanted security risks that come in the form of human errors, malicious insider threats, lack of user understanding of security policies, misconfiguration, etc.

- **FILE SPECIFIC ACTIONS**
    - **File Upload:** Allows multiple uploads in one go
    - **Secure View & Edit:** Has an in-built secure viewer/editor which offers features to view (doc, excel, ppt, pdf, text, images, etc.) and edit your files (word, excel, ppt). It can also be configured to integrate your MS-office, PDF editor, etc. licenses as well
    - **File Move:** This allows a file to move from one folder to another within your isolated Vault
    - **File Delete:** Allows file to be deleted and removed from DataVault. This action always triggers in-session verification workflow and the user must re-verify himself before the action can be performed.
    - **File Download:** Allows a file to be downloaded only after
        - Receiving mandatory download approval from vault owner(s)
        - Then, a link to access the file is sent only to the registered email address of the user who requested the download
        - The downloaded file is encrypted before it leaves DataVault. The system generated key to decrypt the file is separately shared with the user

- **Live Notifications:** All actions performed by the user in a session are displayed to the user
- **Fast & Easy Web Interface Access:** Allows users to access, upload, share files and documents from anywhere, anytime, and on any device

- **SECURE SHARING AND COLLABORATION FEATURES**
  - **File Share:** You can invite others to your vault with granular user action controls and share individual files with them for collaboration
  - **Auto-Expiration:** Access to files automatically expires on a set date
  - **File Locking:** Lock files in edit mode to avoid conflicting changes
  - **Revoke Access:** Revoke user access to shared files anytime
  - **Notifications:** Sends email alerts for different actions performed in the Vault such as user creation, user updated, and various other user actions.

- **ADDITIONAL SECURITY FEATURES**
  - **File Distribution:** No feature to direct download, print, or copy/paste
  - **Audit Trails:** Detailed audit trails (What, When, Who, Where, and How)

DATAVAULT CONFIGURATION

- Each DataVault is pre-configured with a fixed set of isolated and independent Vaults that can be assigned to individuals or business unit
- As per the requirement, DataVault can be configured for intranet or internet access
- Built-in help manuals that provide clear and concise explanations of how to use DataVault features and perform user actions

DISASTER RECOVERY

The following disaster recovery options are available for DataVault:

- Each DataVault instance comes with RAID installed for data redundancy and recovery. RAID can support fault tolerance of one disk failure at any given point in time.

- High Availability configuration can also be set up where another DataVault is installed at the DR site and is actively replicated. In the event of a disaster/failure, the DR instance can be immediately brought up. This will ensure the continuous availability of DataVault services.

DATAVAULT APPLIANCE VERSIONS

DataVault Standard Edition
Per Instance

- 8 TB total storage, 6 TB for DataVault, and 2 TB for redundancy (RAID)
- 15 Vaults
- Up to 60 Vault Users (Owners, users, and guests)
- 15% concurrent users

DataVault Enterprise Edition
Per Instance

- 40 TB total storage, 32 TB for DataVault, and 8 TB for redundancy (RAID)
- 30 Vaults
- Up to 90 Vault Users (Owners, users, and guests)
- 15% concurrent users

TECH SUPPORT

- Inclusive of 3 years product warranty
- Customer support – via Phone and Email
- Incident Response Time: under 30 mins (from the time the issue is reported to Sherpas customer care)

- Incident Resolution Time:
  - Severity 1: 8 hrs.
  - Severity 2: 24 hrs.
  - Severity 3: 48 hrs.

- Online self-help document for quick resolutions of small issues