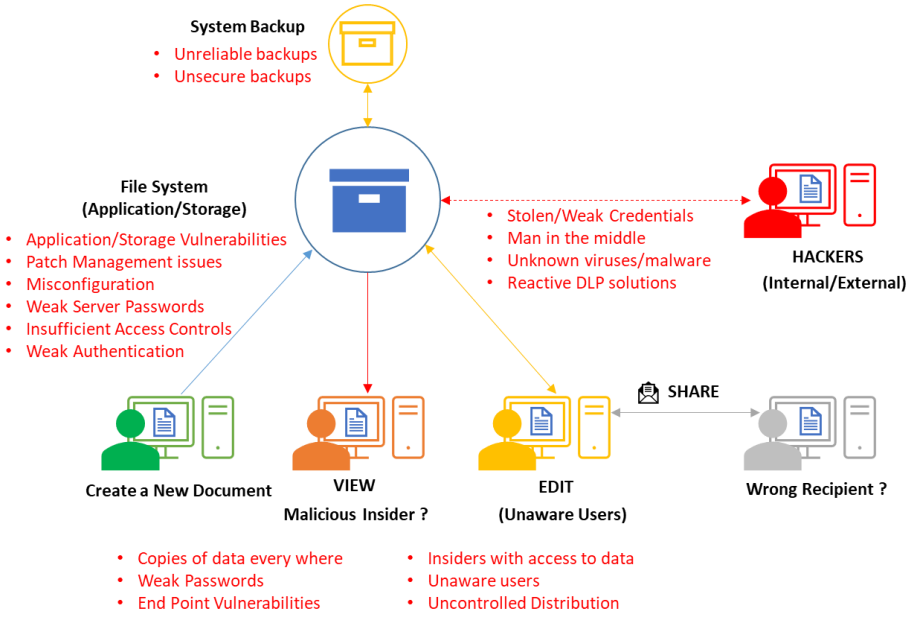
Whitepaper on Centralized Secure Document Repository

INTRODUCTION

With the advent of newer technologies, organizations globally are facing significant cybersecurity risks than ever before to secure their digital assets. They are deploying a multitude of solutions to protect themselves from these cyber-attacks. However, globally they are being hacked - some know that they are hacked, and some do not. According to IBM, in 2019 on average it took organizations about 206 days to identify a breach and 314 days to contain (from breach to containment). The threat is real, solutions are not effective enough and it is not a matter of how, it is a matter of when. In the past few years, we are seeing an increase in state-sponsored cyber-attacks globally. These attacks are much more sophisticated and potent, primarily focused on data theft than disruption. In addition to this, insider threats are increasing by the day and according to CheckPoint's 2020 Cyber Security Report, "*34% of cyber-attacks are perpetrated by insiders, making it clear that legacy security infrastructures, characterized with flat networks, are dangerously ineffective*".

CURRENT CHALLENGE

- Organizations have documents that might contain confidential data.
- Documents containing confidential data have to be protected from unauthorized access, manipulation, destruction, and theft.
- They are typically stored on shared network drives, removable storage devices, endpoints, air-gapped networks, cloud storage, and/or document management solutions.



- Most of these document storage solutions are meant for ease of access and collaboration, exposing the data to numerous threat vectors.
- Organizations need competent cybersecurity personnel to precisely configure, constantly monitor logs and events to ensure that the confidential data is properly secured.

- Endpoints can be easily compromised, and any confidential data stored on these endpoints have a huge cybersecurity risk.
- A genuine user mistake and put the entire data at risk.
- Malicious insiders are constantly looking for opportunities to exfiltrate and/or compromise data.

Solution – A Centralized Secure Document Repository

The solution is to set up a Centralized Secure Document Repository that enables.

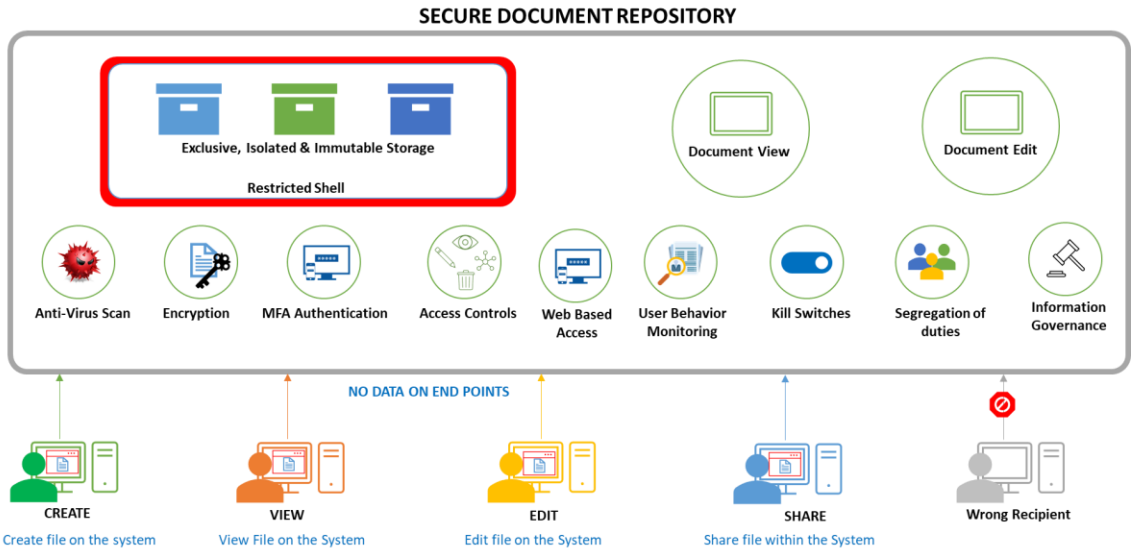
- Secure and immutable storage of data
- Exfiltration Protection from malicious actors (internal and external)
- Timely Exchange of sensitive information
- Strong Security Controls
- Finer Access Controls
- Anytime access to the data from any of the branch offices
- Backup and disaster recovery

New security paradigms are evolving that could enable the setting up of a centralized secure document repository. Below are some of the new paradigms when taken into consideration will provide a defense-in-depth solution.

- **Focus on protection than detection**: The primary focus of the security solution must be on the protection of the data rather than on intrusion detection. The solution must protect data at all times from internal and external threats
- **Trust No One**: System must not trust data requests coming in from anyone or any source or any network. No one is to be trusted. (ISO 27001, NIST SP 800-207)

- **Multifactor Authentication and In-session authentication**: multi-factor authentication with a User ID, password, and TOTP must be enabled for system access by default. User sessions must also be validated for authenticity while in session (ISO 27001:2013, NIST 800-171, GDPR, PCI-DSS)
- **Tighter and Layered Access Controls**: Access controls must be frequently reviewed and must be layered and tamper-proof.
- **Restricted Shells**: Restrict the users to shells with fewer commands to prevent access elevation and lateral movement.
- **Encryption of data at rest and in transit**: Always ensure that the data is encrypted at rest and in transit (ISO 27001:2013, NIST 800-111, HIPAA)
- **No data on endpoints**: Sensitive information must not be transmitted to endpoints. The system must enable the end-users to create a document on the system, view it on the system, and edit it on the system. This eliminates the need for additional security measures on the endpoints for data protection and solves the problem of multiple copies of the data lying everywhere within the organization
- **Secure Web Application Interface**: The centralized secure document repository shall be accessible via a secure web interface and all communication between the client and server shall be encrypted.

- **Anti-Virus Scan**: Ensure that all documents are scanned for viruses before they are uploaded onto the file system (NIST SP 800-82 Revision 1)
- **Control distribution of documents**: While collaboration and information sharing is essential, ensure that the document is shared within the system, for a fixed period and with only permissions as required. Users to whom a document is shared will be able to access the document on the system after login in. Even in this case, the document is not physically shared with the end-user
- **Monitor User Behavior**: Monitor user behaviors to identify potential end-users with malicious intent.

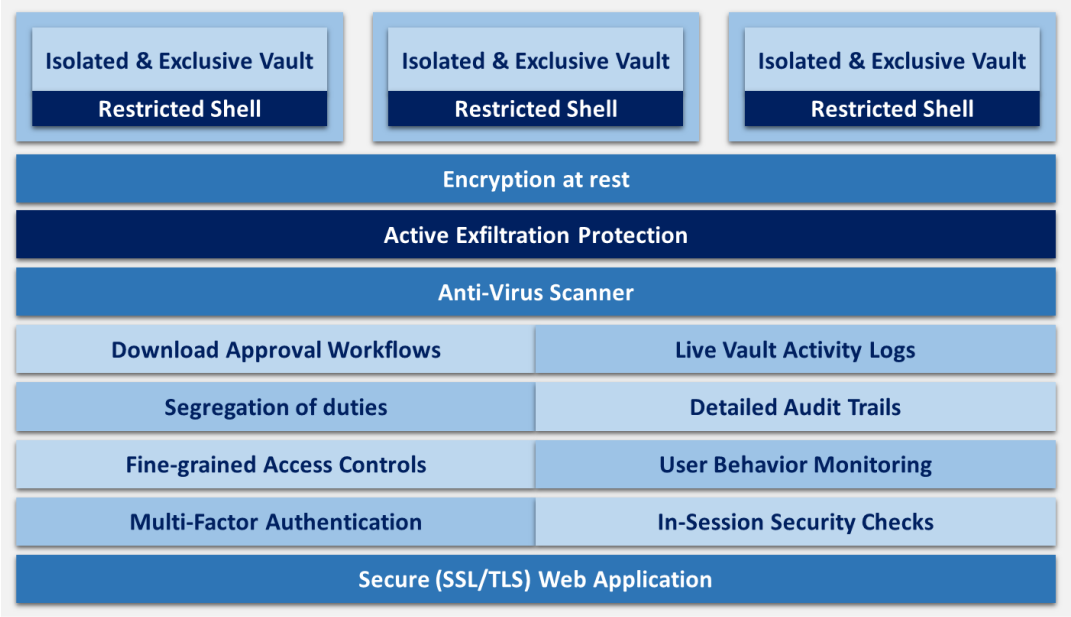


- **Immutable Storage**: Always store sensitive data in immutable storage to ensure that the data is not manipulated by unauthorized personnel.
- **Exclusive and Isolated Storage Pools:** System must segregate the storage area into exclusive and isolated storage pools that only the users of a specific business function/department will access. The storage pool allocated to this group of users must be in the exclusive possession of this group alone and no one will be able to access its contents, even while the rest of the storage pools are all on the same storage
- **Information Governance**: Ensure that basic information governance guidelines like data ownership and approvals are implemented to provide complete control and ownership of the data to the respective storage pool owners. No document shall be downloaded without the explicit approval of all the data owners
- **Audit Trail**: Ensure that detailed audit trails are maintained for all user actions (HIPPA, GLBA, ISO 27001, FISMA, GDPR, PCI DSS)
- **Kill Switches**: System must have kill switches to enable quick disabling of user access (even while in session) and isolation of file system
- **Segregation of duties**: Ensure that the administrators do not have access to the data in the file system that they are administering.

- **Backup and Disaster Recovery**: Deploying the secure storage repository in high availability mode and enabling secure backup as per the organization's policy to implement disaster recovery and business continuity.

OUR DATAVAULT SOLUTION

Our patented DataVault solution is built on these new paradigms of security. DataVault is built with a security-first approach and has an amazingly simple and intuitive user interface for easy access and collaboration. DataVault has layers of security precisely configured to ensure that there are no white spaces in between that can be exploited to gain unauthorized access to the underlying storage.

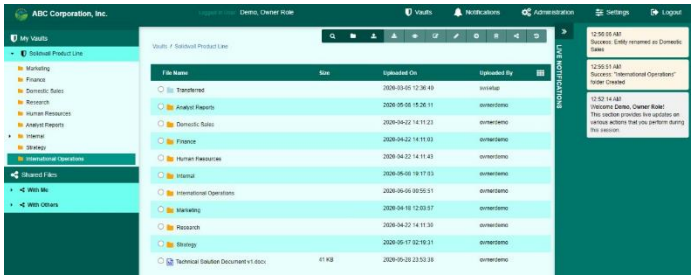


DataVault can be offered as an appliance with its own secured storage space which could be tightly controlled and protected. But in scenarios where securing existing storage is a requirement, DataVault can be offered as a software solution for protecting on-premise data storage. Apart from that, DataVault can also be offered as Software as a Service in the cloud. With these different options, DataVault can seamlessly fulfill various customer requirements and needs around secure, scalable storage.

Below are some of the most important security features of DataVault

- Secure and immutable storage for document storage. Entire storage is segregated into mutually exclusive and isolated vaults so that different user groups within the organization can use the same storage as a stand-alone secure document storage solution.
- Layers of security expertly configured to minimize threat vectors.
- Unbreakable restricted shells that limit the users to a limited set of commands
- Data cannot be downloaded by default from the DataVault system.
- Data is encrypted at rest and in motion.
- Secure File Viewer/Editor to securely view or edit documents right on the DataVault system. There will be no data on the endpoints.

- Adaptive Multi-Factor Authentication not only ensures users use Multifactor Authentication at the time of login but also validates user authenticity during the session based on user behavior and/or specific actions.
- Securely share documents with different people within and outside the Organization without ever taking the document out of the DataVault system



BENEFITS OF DATAVAULT SOLUTION

- Secure, Isolated, Exclusive, and Immutable Vaults
- Bute force entry protection
- Insider threat protection
- Protect confidential files from unauthorized access, manipulation, destruction, and/or theft.
- All layers are expertly configured, which eliminates misconfiguration issues.
- Restricts unauthorized download of data.
- View, Edit, Share documents right on the device. No data on endpoints
- Do not allow printing of documents.
- Detailed activity logs capture all user actions.
- Easy to use, administer and maintain.
- Enable quick compliance to various statutory requirements.
- Options for installation on-prem or on cloud or as an appliance

CONCLUSION

Some of the most reputed and large organizations (including many tech companies) around the world have been victims of data theft in the recent past. Traditional centralized document repositories have too many inherent security-related issues which have been exposed time and again, and data has been stolen/manipulated/destroyed. Considering the scale and sophistication of cyber-attacks, a new approach to document protection must be the need of the hour. A defense-in-depth solution with multiple layers of security placed right where the data resides is essential.

DataVault system is built with security first and easy user interaction. DataVault offers superior security features when compared to any other secure document management solutions available on the cloud or on-premises.