CyberVault Secure Data Room Solution

In today's rapidly changing and increasingly mobile business world with vast threats for any digital asset and increasingly remote workers, companies must quickly adjust their security measures from static security within firewalls to enhanced mobile security exactly where information is being created, modified, or transferred. We are during the age of the knowledge worker where information needs to be at hand, no matter where, when, or on which device. Knowledge workers also collaborate with distributed team members, contractors, partners, suppliers, and vendors from wherever they are, which is a massive challenge for IT managers and compliance officers.

To cover the needs of effective and dynamic document collaboration and still protect a company's information, enterprises must make sure the solution they choose does not just focus on seamless collaboration but also has a solid commitment to protecting confidential content.

The CyberVault Secure Data Room is a single platform that resolves the challenges of protecting confidential documents and facilitating efficient workflows that enable internal and external collaboration. CyberVault's platform helps companies meet legal and regulatory compliance — including the DFARS, EAR, and ITAR — with transparent, traceable processes. At the same time, employees can access, work and securely share corporate files on mobile devices anywhere and anytime.

Security: End-to-End Protection for Important Documents

Two-Factor Authentication and Access Permissions

Along with the flexible permission system and the high-security two-factor authentication — based on emails and tokens, companies can accurately define and monitor access, roles, and permissions for the members of a data room.

Highly Secure Document Encryption

Set as a standard configuration, the high-security, 256-bit AES encryption on the server provides effective protection for all documents and prevents them from being accessed by unauthorized users, including IT service providers and administrators. All of the data transmitted between the client and the server (document and file upload or download and display of Data Room content) is protected with 256-bit SSL encryption.

Secure, Traceable Delivery

Documents are not sent out as attachments. Instead, the user receives an email containing a link to the document in the CyberVault Secure Data Room. Documents can also be sent to users who are not members of a Secure Data Room via external links. These links give users secure access to a document in a Data Room for a limited time only. This method avoids the need to send users non-secure email attachments. The audit trail can log the whole download, editing, and distribution process.

Integrates Virus Scanner

Documents are checked for viruses during the upload process and, if necessary, they are isolated and automatically prevented from being uploaded.

Encrypted Emails

The email text is also encrypted, providing additional protection for company communications. Depending on the recipients' profile, they receive the email encrypted with a simple message alerting them that a new document has been added to the Data Room.

Integration for Microsoft Outlook

The Secure Connector for Outlook is installed on a users accessing device and subsequently appears in Microsoft Outlook as an add-in. It provides a quick and easy yet secure way for users to send documents to people inside and outside the company. The add-in ensures that information is stored in a Secure Data Room instead of being sent insecurely as email attachments. The recipients of a message will receive an email in which those attachments have been replaced by links to the documents, which are stored in the Secure Data Room. The email text itself is also stored in the Data Room as a message object and linked to the uploaded file. Users can also securely store older emails and attachments they have already received.

Your Benefits At A Glance

- Consistent protection of confidential documents — from one end to the other.
- Traceability of data room communications.
- Complete, yet flexible, protection of confidential email content.
- Highest levels of security with strong authentication and encryption of data transmission and storage.
- Fulfills compliance requirements with integrated tamper-proof audit trail.
- Integrated document management.
- Operator shielding — administrators and IT service providers cannot access data room content.
- Intuitive and user-friendly.
- Any data room content is available at any time or location using a web browser.

Personalized Homepage

Users can choose the layout of their personalized homepage to suit their needs: view all the Data Room activities at a glance, including status changes to documents, as well as received and sent emails. If users prefer, they can choose an overview of all messages, or go directly to a specific folder when they log in.

Collaboration Center

The Collaboration Center provides direct access to received and sent messages. All communication items are marked with a specific completion status that shows which emails are still in progress.

Integration in Microsoft Office

Users can access Data Room folders via Windows Explorer. They can open and edit Microsoft Office documents directly with the corresponding application and, with one click, save them back into Data Room. This function provides full support for versioning, access control, modification tracking, and encrypted data transmission.

Add Links to Data Room Items

Users can add links to Data Room items (i.e., documents) and folders within the same or another Data Room.

Upload Files as Zip Files

To upload a folder, including its sub-folders and contents, or a large number of documents in a single operation, you can compress them into a zip file and then upload it to the Data Room. Empty folders in the zip file are created in the Data Room as well.

Compliance: Fulfilling Internal and External Regulations

Secure Document Viewer

The patented and integrates Secure Document Viewer prevents documents from being downloaded from the Data Room. The full content of the original file is never displayed on the user's local accessing device. Instead, the user views the pages one at a time as tiled images in the browser. This eliminates the risk of unauthorized downloads. No confidential data remains on the user's accessing device once the session is over.

Operator Shielding

Confidential documents can be protected from access by internal or external IT administrators due to the complete separation of application and systems administration duties, as well as the integration of two-person approval processes for all security-related administration functions.

Tamper-Proof Audit Trail

All actions on the application, Data Room, and object levels can be time-stamped and recorded in a tamper-proof audit trail. These actions usually include configuration changes as well as document access, editing, and the addition of new documents to a Data Room. The display of individual pages in the Secure Document Viewer is also logged in the audit trail. Users are only able to see information for which they have viewing permission. Further actions, such as downloading documents, can be recorded separately. Customers can also limit access to the audit trail itself and the application ensure that it cannot be altered later.

Watermarks

Watermarks are generated dynamically and provide documents with additional protection against unauthorized forwarding. The content and layout of the watermark are fully configurable. For example, the user's name can be automatically embedded in the background of each page.

Data Room Index

The index lists all the items in the Data Room in chronological order. The list is fully configurable and can include the item's description, size, owner, and other information. The result can be downloaded as a pre-configured Excel file.

Brainmark ID

The Brainmark ID is a unique identifier that is added to every page of a Brainmark document.

What is a Brainmark?

A Brainmark-secured download delivers an automatically generated and protected version of a document to the user. The sender can select from the following security options:

- The document has a unique identifier using digital fingerprint technology.
- The document is delivered as a simple but clearly marked print version with all edits removed.
- The document is delivered with a personalized watermark.
- The user can only view the document, not forward or print

Administration & Configuration

Globalization

To simplify collaboration between users' locations in countries with different languages and time zones, the CyberVault Secure Data Room Service automatically detects the language and time settings of the user's work environment or browser when they register and adjusts the display accordingly. This setting can be adjusted by each licensed user.

Retention Periods

To make sure that folders and documents are not stored in the Data Room for longer than necessary, Data Room Managers can define a retention period in days for which these items should be retained.

Data Room Center

The Data Room Center facilitates the centralized management of Data Rooms, users, Data Room templates, logos, and style sheets. Data Room Center administrators can create as many Data Rooms as required.

Data Room Templates

Data Room templates make it quick and easy to set up a new Data Room with preconfigured content and parameters, including specifications for roles, permissions, folder structures, security, and authentication policies.

License Management & Storage

Data Room Center Managers can adjust the number of users and ordered storage for their Data Room Center and its Data Rooms on their own.

Data Room Operation

ISO/IEC 27001:2013 Certification

The International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC) have certified CyberVault's hosting provider Amazon Web Services (AWS) as ISO/IEC 27001:2013 compliant in terms of secure operations of all SaaS platforms in accordance with the statement of applicability.

Data Security

Subject to customer's choices, a security copy of every Data Room is made once a week. These weekly backup copies are available online for 30 days, or longer if requested. In addition, customers can request a complete backup of a Data Room daily or another periodic basis, if required.

FedRAMP Certification

CyberVault's Secure Data Room Service assures users of FedRAMP (Federal Risk and Authorization Management Program) platform certification for all important, confidential, and other information through its FedRAMP certified hosting provider.

DFARS/ITAR/EAR Compliance

The CyberVault's Secure Data Room Solution establishes compliance with the DFARS, ITAR, and EAR through both assessment and certified hosting provider services.

Secure Data Center Operation

The application is operated within certified data centers. The strict separation of the application and system administration functions ensures that documents cannot be accessed by administrators working for the application service provider. Servers are located in the U.S. enable customers to store their data safely and securely.

Examples of Processes that Require Confidential Documents to be Protected:

- Communications between Project work involving several management and board members companies.
- Mergers and Acquisitions Life Sciences out-licensing
- Global collaboration with partners Preparation of quarterly, annual, and customer reports.
- ITAR/EAR/DFARS compliance Due diligence.