Virtual StrongBox Security

How Virtual StrongBox provides unmatched security and convenience

VIRTUAL STRONGBOX ANSWERS THE TOUGH CLOUD SECURITY QUESTIONS	
Where is my data?	Your data is stored in our private data centers. In the United States, data is stored in Charlotte, NC and replicated off-site to Little Rock, AR. We have a separate data center for Canadian clients, located in Toronto, to maintain data sovereignty. Virtual StrongBox uses SSAE 16 Type II accredited datacenters to host the SaaS application and metadata. All files are stored in SSAE 16 SOC 1 and SOC 2 accredited datacenters with high availability and durability ratings.
Can I permanently delete my data?	Yes. When a file is deleted, it is permanently deleted from our production servers.
How is my data stored?	All data is encrypted in transit and at rest in our environment.
Who else can see my data?	Only the Virtual StrongBox owner can see files placed in their personal StrongBox. Virtual StrongBox employees do not have access to a client or customer files. Administrators do not have visibility of their customers documents until granted permission.
How do I get my data back and avoid vendor lock-in?	Virtual StrongBox clients can call our account managers at any time to remove their data and avoid vendor lock-in.

Virtual StrongBox Security

How Virtual StrongBox provides unmatched security and convenience

Feature	Description
Data Security	
Total information privacy	Only the Virtual StrongBox owner can see files placed in their personal StrongBox. Virtual StrongBox employees do not have access to a client or customer files. Administrators do not have visibility of their customers documents until granted permission.
Datacenters	Virtual StrongBox uses SSAE 16 Type II accredited datacenters to host our SaaS application and metadata. All files are stored in SSAE 16 SOC 1 and SOC 2 accredited datacenters with high availability and durability ratings.
Encryption	Patented methods of encrypting files in transit and at rest using AES 256-bit encryption, a Federal Information Processing Standards (FIPS) encryption algorithm (FIPS 197).
Security Patents	Virtual StrongBox has three patents (as of 2016) for our encryption and security measures.
Firewalls	Files are processed using systems protected by securely configured firewalls that effectively limit and control access to network segments.
Redundant Storage	Files are stored and replicated with leading Infrastructure-as-a-Service (IaaS) providers to ensure high file durability and availability
Backup and disaster recovery	Data is backed up and replicated to another data center to ensure continuity.
Multi-factor Authentication Client level	Clients may set up a multi-factor authentication process that requires the submission of the account password and a secondary authentication, such as a SMS text message, in order to access their StrongBox.
Multi-factor Authentication User Level	Users can turn on a multi-factor authentication process that requires the submission of the account password and a secondary authentication every time they login.
Access log retention	Detailed file-access logs are retained indefinitely.
Audit Controls	Clients can use the tools provided within Virtual StrongBox to review account activity, such as account usage and access to files.

Account Lockout	Virtual StrongBox will lock customer out of their account after five invalid logon attempts to prevent account tampering. Customers can reset passwords using their email.
Timed Logout	Virtual StrongBox will automatically log users out after 20 minutes of inactivity.
Password Settings	All passwords have an eight character minimum, which must include letters, numbers and a special character.
Role-based Administration	Administrators can set different level of roles to employees to limit access to certain functionality.
Configurable settings	
SAML enabled single sign-on	Virtual StrongBox supports SAML 2.0 for single sign-on and integrates with most SAML-compatible identity management solutions.
Portal Customization	Clients can provide Virtual StrongBox through a secure portal, turning on Multi-factor authentication for additional security.
Terms and conditions	Terms and conditions are displayed when users register for Virtual StrongBox, then accessible inside Virtual StrongBox thereafter.
File restriction	Clients can restrict certain files types from being exchanged in Virtual StrongBox.
Data protection during document exchange	
Direct exchange using API	Virtual Strongbox employs TLS protocols to protect client/user authentication, authorization and file transfers in whatever application best fits the client.
Secure Link Creation	Virtual StrongBox download and upload links are uniquely and randomly generated using strong authentication codes.
Additional link privacy settings	Unique links can be given pin codes, expiration dates and limit to the number of clicks on a specific link (one-time only or multiple).
Trusted advisor drop files with shared folder	Upload links can be shared with a trusted advisor so files can be dropped into a users Virtual StrongBox.
Data protection during document storage	
Understand data location	Clients know exactly where their data is stored, as well as who has access to their data.
Permanently delete data	When data is deleted within Virtual StrongBox, the data is not recoverable.
File Size Limits	Clients decide how large files placed in Virtual StrongBox can be.
Testing and evaluation	Virtual StrongBox engages with a third parties to perform periodic risk assessments and gap analyses.
File Archiving	Virtual StrongBox supports your compliance with federal regulations regarding data retention by retaining all user actions.