SECURE YOUR DATA EXCHANGE WITH SAFE-T BOX

SAFE-T BOX WHITE PAPER

SAFE-T
Smart Security Made Simple.

1 The Costs of Uncontrolled Data Exchange 3
2 Safe-T Box Secure Data Exchange Platform 3
2.1 Business Applications and Data Connectors 4
2.2 Automated Security Policy Enforcement Engine 4
2.2.1 User Authentication 6
2.2.2 Data Scanning 6
2.2.3 Data Encryption 6
2.3 Secure Transfer Solutions 7
2.3.1 Secure Email 7
2.3.2 Secure Managed File Transfer (MFT) 8
2.3.3 Secure File Sync and Share (FSS) 8
2.3.4 Secure Data Exchange Network 8
2.4 Anytime, Anywhere Access 9
2.5 Fully Managed 9
2.6 Designed for Regulation Compliance 10
2.7 Eliminate Sensitive Data from the DMZ 10
3 Solution Benefits 11
4 Summary 11

1. The Costs of Uncontrolled Data Exchange

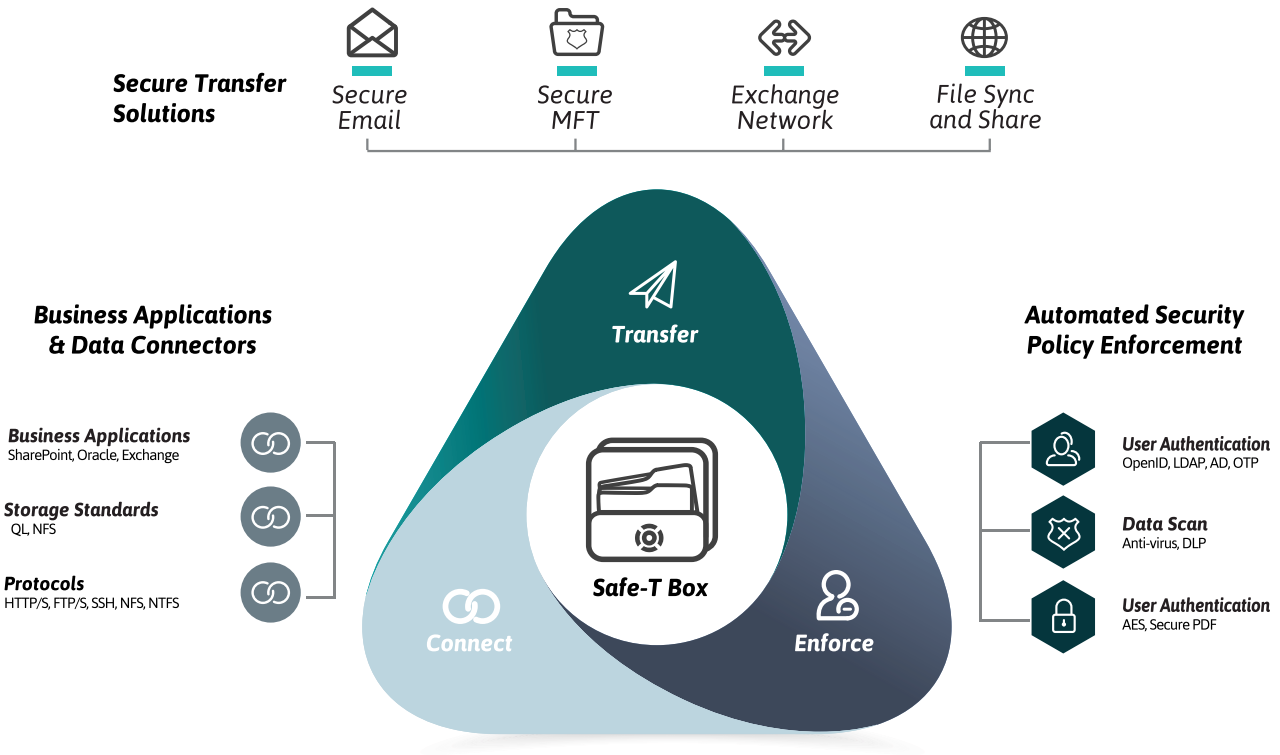
Today, email is the most common method of exchanging data between users, business partners and customers. According to a research conducted by the Radicati Group , in 2013 105 billion business emails were sent and received daily, which is expected to grow to over 130 billion in 2017. As well as emails, business users also transfer files using a variety of other methods including FTP and cloud storage solutions such as Dropbox, Google Drive and SkyDrive. It is clear that a large amount of business data is transferred out of the organization each day.

While not all transferred files are confidential and sensitive, statistics show that almost 40 percent of business users have shared sensitive data using email or other file transfer methods. This means that many organizations today are unknowingly in breach of regulations and are potentially at risk of liability claims and public defacement, due to sensitive data leakage.

To greatly reduce the leakage of sensitive and confidential data, IT organizations should strengthen their control of shared data by offering their users a secure, simple to use data exchange solution. Such a solution must become the standard method of sharing data within the organization as well as with external business partners, customers and suppliers.

2. Safe-T Box Secure Data Exchange Platform

Safe-T Box enables organizations to control and secure data exchange of any type and size between people, applications and businesses. Built on the industry's widest range of pre-configured application connectors and powered by an automated security policy enforcement engine, Safe-T Box is designed to rapidly add security and control across a wide variety of data exchange scenarios within the organization. Safe-T Box enables organizations to quickly and easily add security layers to existing business processes, to strengthen the control of and reduce the costs of sensitive data sharing. Safe-T Box's unique modular architecture and integration capabilities ensure that it seamlessly integrates into existing data exchange scenarios in the enterprise, providing policy enforcement and secure data transfer.



Safe-T Box Secure Data Exchange Platform

Safe-T Box is comprised of three separate, yet interconnected modules:

- Business applications and data connectors
- Automated security policy enforcement engine
- Secure transfer solutions

2.1. Business Applications and Data Connectors

Safe-T Box support dozens of pre-built Safe-T Connectors divided into three types:

Business Applications	Storage	Protocols
• SharePoint	• SQL	• HTTP/S
• Oracle	• MySQL	• SSH
• MS Exchange	• NFS	• FTP/S
• Salesforce	• NTFS	• etc
• IBM AS400	• SSH	
• etc	• Cloud Storage	
	• etc	

By utilizing Safe-T's connectors, Safe-T Box offers the industry's most integrated data exchange platform, allowing applications to securely share sensitive data with users and other applications across a variety of enterprise and cloud storage solutions.

To ensure simple integration with the organization's business applications, Safe-T Box provides the unique capability of pulling data from applications, local and network folders and storages. Safe-T Box continuously polls a pre-defined location and once a new file is placed in the folder, Safe-T Box retrieves the file

This tight integration between Safe-T Box and the organization's business applications, allows the applications to easily check-in and check-out sensitive data to/from folders across the network or from/to any application or storage location, without requiring modifications to the applications' code, eliminating the need for IT staff to perform systems integration typically required by other data exchange solutions.

2.2 Automated Security Policy Enforcement Engine

Safe-T's policies enforcement engine allows enterprises to add security layers to existing data exchange processes easily and quickly. The shared data is fully controlled and monitored, providing complete auditing and tracking of who accessed data and when. It allows to automatically enforce security policies on incoming and outgoing shared data.

The user can create policies and procedures for content sharing that can be integrated intuitively into streamlined work flows. The platform provides collaboration with security platforms of industry-leading enterprise security solutions, such as Anti-Virus, DLP, FLP (File Level Permission), User Rights Management, or any other third party security solution by connecting via its API/Command Line.

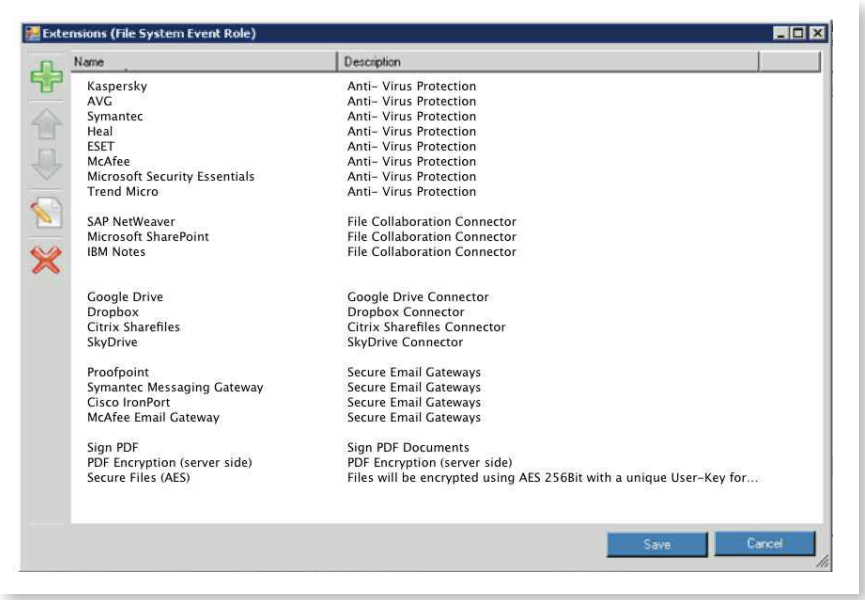


Figure 2 - Security Policy Enforcement Engine Connectors

To create a new policy, the user need only access the relevant storage or folder, and choose the relevant enforcement actions. As can be seen in Figure 3 below, the user defined that any file placed with the Secure PDF folder, should be encrypted using the Secure PDF and AES methods.

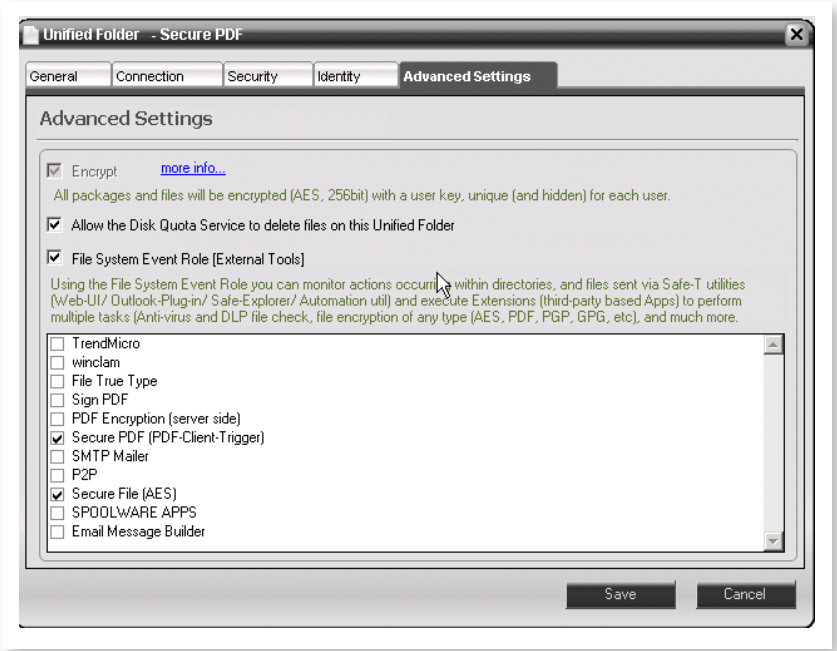


Figure 3 - Security Policy Enforcement Engine - Rules Interface

The policy engine supports four types of enforcement actions:

User Authentication	Data Scanning	Data Encryption	Other
• LDAP • Active Directory • OTP • Open ID • SAML	• DLP • Anti-Virus • Gate Scanner	• AES • Secure PDF	• Customized automation processes

2.2.1 User Authentication

User authentication enforcement actions can be performed as part of policies applied to incoming traffic, e.g. it authenticates a user trying to download a file, or outgoing traffic, e.g. it validates that a user can upload a file to the cloud.

In addition to the authenticating users via the organization's LDAP or Active Directory systems, Safe-T Box supports three unique authentication mechanisms:

- **One Time Password (OTP) -** one-time passwords are sent in a separate email or text message (SMS), to the recipients in order to grant access to the file.
- **Open ID -** Safe-T Box enables authenticating either registered users or ad-hoc users using the user's existing personal social network credentials including all common social networks, such as Facebook, Google, Live ID, etc.
- **Any users DB -** SQL, MYSQL, Oracle, CSV/XLS files, etc.

2.2.2 Data Scanning

In order to ensure only approved files are transferred in and out of the organization, Safe-T Box supports a variety of data scanning enforcement actions.

Safe-T Box can pass traffic via a variety of third party DLP (data leak prevention) engines, ensuring confidential files are not transferred out of the organization.

For incoming traffic, Safe-T Box can pass traffic via a variety of third party Anti-Virus engines as well as Sasa Software's Gate Scanner solution and more.

2.2.3 Data Encryption

Safe-T Box can encrypt files before they are shared with recipients. Encryption is done either using the built-in AES and PDF Encryption modules, or by passing the file via third party encryption engines or any custom encryption algorithm.

The files are encrypted prior to placing them in Safe-T Box secure storage using a powerful minimum AES 256 file level encryption, ensuring they are also secured during rest until they are downloaded.

Files are also secured during download, by using secured protocols such as HTTPS, FTPS, SFTP and SSH between Safe-T Box and the recipient.

Examples of popular security policies created by customers:

- **Outgoing data** should be authenticated, scanned with DLP and encrypted to ensure only approved data is shared securely.
- **Incoming data** is authenticated, decrypted and scanned for viruses and malware before it is approved for sharing with people and applications within the organization.

2.3 Secure Transfer Solutions

Safe-T Box offers multiple innovative solutions to securely transfer shared data to an authorized destination:

2.3.1 Secure Email

Safe-T Secure Email empowers enterprise users to send encrypted emails securely to customers and business partners. Emails can be sent to anyone without disrupting the normal routine by not requiring the recipient to install software or exchange keys. Business users can send encrypted emails of any size and type to registered or ad-hoc recipients, providing a simple, easy to use and fully auditable alternative to PGP.

Secure Email works as follows:

1. Once the encrypted email and its attachments are sent, they are stored in the Safe-T Box server of the sending organization.
2. The recipient receives an email with a link which is clicked on to retrieve the stored email at the sender's organization.
3. Using either a one-time password or oAuth2 (Live ID, SAML) username and password, the recipient is authenticated and can then access the encrypted email and download any attachments via the organization's portal.

Safe-T Secure Email has two main deployment options:

1. **Safe-T's Outlook plug-in** - enterprise users can conveniently send files of any size directly from Outlook, using their existing email routine. The plug-in is packed with a generous array of file transfer options, tracking capabilities, and management controls, according to the permissions assigned by enterprise IT.
2. **Safe-T Secure Email's LNK Connector** - allows enterprises to monitor and handle incoming and outgoing email messages. LNK connector is a SMTP gateway deployed as the next hop email server "before" or "after" the organization's existing mail server. Once LNK connector "catches" an email message, it scans the message attributes including the message subject, body, header, attachment type and size; then, based on pre-defined rules, LNK connector performs the required action for example, encrypt, drop, forward, etc

2.3.2 Secure Managed File Transfer (MFT)

Safe-T Secure MFT allows enterprises to securely transfer sensitive data outside the organization with a secure, user-friendly FTP replacement solution. Integrating seamlessly with business applications, legacy systems and proprietary tools, the secure MFT solution adds security layers to standard file share solutions including authentication, data scanning and data encryption.

2.3.3 Secure File Sync and Share (FSS)

Safe-T Secure FSS is a robust and secure enterprise Dropbox solution, enabling business users to securely share with business functions and business partners across the globe from any device.
Safe-T Box is comprised of multiple secure folders, which can be associated to a specific user, or group of users. All users' data, uploaded or received is stored in a secure folder, which can either be local or network folders (e.g. FTP, SFTP, SQL, SSH). Communication between the folders is done using standard secured protocols ensuring end-to-end security without requiring proprietary protocols.

2.3.4 Secure Data Exchange Network

Safe-T Secure Data Exchange Network enables organizations to create a secure 'internal' network of secure storages, where they can easily and securely transfer files of any type or size to and from their company headquarters to business partners, suppliers and customers.

Once deployed, business users have instant access to all authorized folders and files, enabling them to exchange files using an interface similar to desktop file system interfaces they are familiar with.

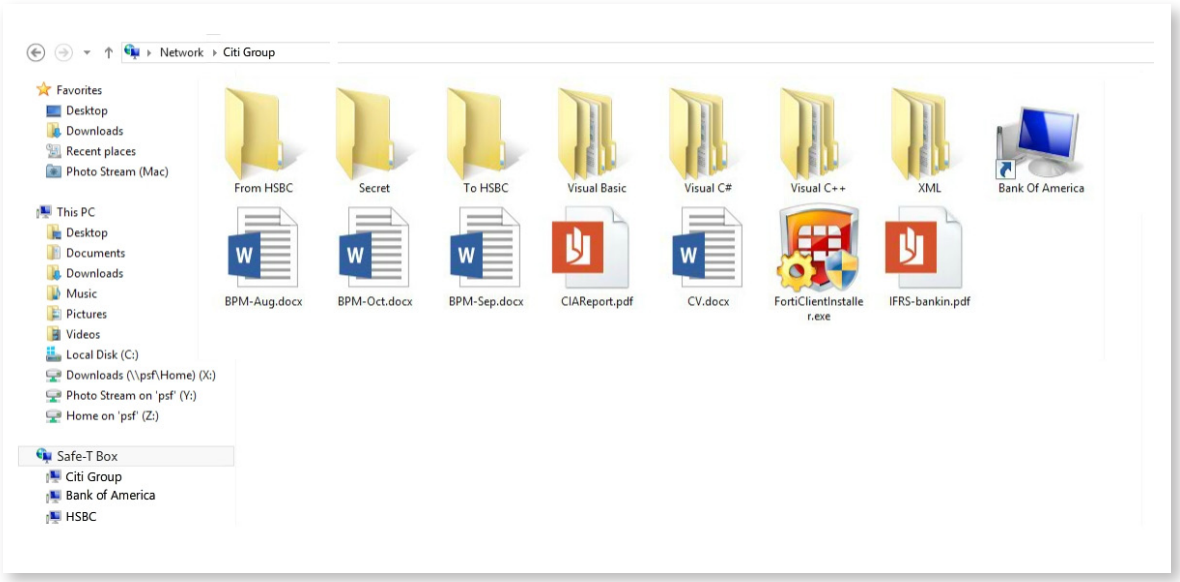


Figure 4 - Secure Data Exchange Network - User Interface

2.4 Anytime, Anywhere Access

Safe-T Box allows users, whether they are business users, business partners, or ad-hoc users to access files and data from a variety of interfaces:

- From within Outlook using a simple and user-friendly plug-in
- Via a browser using Safe-T's simple web user interface that is available from any Internet-enabled computer or mobile device supporting HTML 5.
- From a desktop using Safe-T's Safe Explorer software

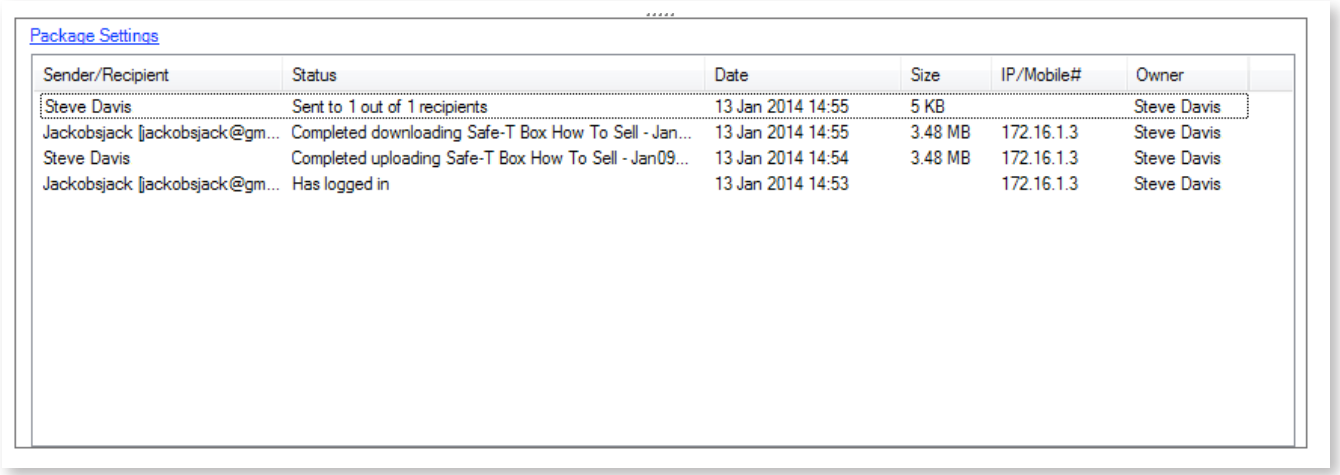
Within the user interfaces, users can perform the following operations -

- **Share any file type or size –** Users can share any file size and type.
- **Powerful and flexible security levels -** Users can select the associated security measures for each shared package containing sensitive data and files.
- **Self-managed tracking, with access to a range of file-level capabilities -** Users can request an automated delivery receipt as well as tracking information regarding the exact time at which recipients downloaded the files.
- **One-time passwords (OTP)-** OTP can be generated and sent in a separate email or text message (SMS), to the recipient in order to grant access to the file.
- **Sent attachments expiration dates -** Users can choose to set an expiration date for sent attachments, after which the files will not be available for download.
- **Read/write and download permissions -** Users can define the email as read-only and limit the availability of attachments to a controlled number of downloads.
- **Allow recipients to respond to the sender -** Users can send an email invitation to the recipient to exchange data without requesting a client installation or registration process.

2.5 Fully Managed

To ensure sensitive data and files are not leaked by employees and in order to be able to track down rogue users (as required by regulations), Safe-T Box enables organizations to easily maintain comprehensive records of their file transfer activities.

Safe-T Box documents key "where, what, who, and when" tracking data for each transferred file. Comprehensive download tracking information is also available, with logs that record the date, time, and IP address of each instance of file access and download. In addition, Safe-T Box provides integration with leading SIEM solutions, allowing it to pass tracking data and logs to the SIEM.



2.6 Designed for Regulation Compliance

Safe-T Box has been designed from the ground up with compliance as a top priority, enabling enterprises from various sectors including financial, healthcare and federal institutions, to comply with over a dozen regulations such as PCI-DSS, HIPAA, FISMA and others to protect sensitive data in transit and at rest.

2.7 Eliminate Sensitive Data from the DMZ

In addition, Safe-T Box includes RSAccess patented technology that offers an additional layer of security by enabling organizations to place shared data within the internal network rather than the DMZ, eliminating the need to open incoming ports within the firewall, and further reducing regulation compliance efforts.

Safe-T's RSAccess Front-End solution is a two-tier deployment:

External RSAccess Node – installed in the DMZ segment

Internal RSAccess Node – installed in a LAN segment

The role of the external RSAccess node is to act as a front-end to all services published within the DMZ. It operates without the need of opening any ports within the external firewall and ensures that only legitimate session data can pass through into the LAN.

The role of the internal RSAccess node it to pull the session data into the LAN from the external RSAccess node, scan it using various application level security techniques, and then pass it to the destination application server.

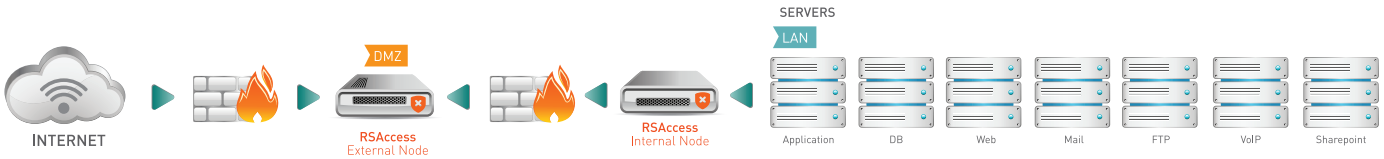


Figure 5 - Safe-T RSAccess Solution

RSAccess provides the following security protection layers:

Blocks Layer 3 and Layer 4 level attacks - complete blocking of any network or Layer 4 based attacks such as port scanning, ICMP scanning, TCP based attacks, etc.

Blocks Application level attacks - RSAccess built-in application level protection inspects and controls incoming traffic on the application layer to detect and mitigate attacks of viruses, Trojans, and malware both on clear channels and encrypted channels such as HTTPS.

Prevents hacking attempts into RSAccess – Safe-T's unique listener technology, prevents hacking into and taking control of the external RSAccess itself to initiate attacks.

3. Solution Benefits

- Data is protected in motion and at rest
- Large files are handled with no exception
- Strengthen control of shared data
- Achieve compliance quicker and in reduced costs
- Easily add security layers to existing business processes
- Complete integration with existing business applications and security tools

4. Summary

Safe-T Box provides a robust platform which empowers IT organizations and security teams to manage and control the data transferred into and out of the organization. With its dozens of Safe-T Connectors, unique policy enforcement engine, and secure transfer solutions, Safe-T Box offers the most cost effective, simple and secure, data exchange solution in the market.

SECURE YOUR DATA EXCHANGE
WITH SAFE-T BOX

About Safe-T

Safe-T is a provider of secure data exchange solutions for a wide range of industries including financial, healthcare and manufacturing organizations.
Safe-T Box, enables organizations to share data securely between people, applications and businesses and is designed for fast and easy deployment and wide user acceptance.
Safe-T's secure front-end solution RSAccess, eliminates the need to store sensitive data in the DMZ, thereby reducing exposure to data breaches. With offices in North America, Europe and Asia, Safe-T secures millions of files and emails every day.

For more information, visit www.safe-t.com.