SAFE-T

Keeping Data in the Right Hands

Secure File and Email Access

Product Brief

Contents

Introduction

Recent research shows that 25% of data is stolen or leaked from organizations via E-mail and file transfer protocols. And within this large amount of data, roughly 43% was due to internal employees (either intentionally or by accident), and 57% was due to external hackers.

Your data is the lifeblood of your organization. Unfortunately, it's continuously at risk of getting stolen or compromised. By nature, your organization has countless methods of accessing files, and they are stored in numerous locations (on premises or in the cloud). This huge proliferation of file access methods and data storage solutions include: cloud storage solutions, S/FTP servers, network file storages, data vaults, document management applications, etc.

In addition, to provide your remote employees, customers and business partners access to files and data, you use various solutions such as email, file distribution applications, EFSS solutions, MFT solutions, etc.
Ask yourself this - once you have large amounts of data exchanged and stored in many locations, as well as many data exchange flows, how do you ensure all data is controlled, managed, and secured. For example, email is the most common method of exchanging data between users, business partners and customers.

Many businesses do not effectively control or monitor their sensitive and valuable data, when accessed, used or transferred. This creates the risk confidential information will fall into the wrong hands. Exposure of confidential information can result in failure to meet regulatory standards (such as HIPAA, GDPR and PCI DSS), legal action, fines, theft of intellectual property, bad publicity, and loss of strategic customers.

Although not all messages and transferred files are strictly confidential, statistics show that almost 40 percent of business users have violated company rules by maliciously or inadvertently sharing 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 large liability claims due to sensitive data leakage.

The Safe-T Solution

Safe-T® Software Defined Access has been designed from the ground up to protect the organizations' files from internal or external unauthorized access, thus preventing attackers from leaking, stealing, misusing, encrypting or compromising your files.

It enables organizations to control access and secure the exchange of any type and size of file between people, applications, cloud solutions, and businesses. It is designed to rapidly add security and control across a wide variety of workflows for enterprises of all types including to and from the cloud.

Built on Safe-T's Software Defined Perimeter technology and Integrated Data Security Platform, and Safe-T's unique Secure Virtual Vaults (SVV) technology, it creates the only true Secure File and Email Access solution.

How It Works

As can be seen in figure 1 below, the Safe-T Secure File and Email Access is composed of three access servers. The solution is deployed in multiple tiers within the organization and cloud:

- **DMZ tier** – includes an Access Gateway which is located after the WAN firewall
- **Anti-Malware tier** – includes an Access Controller, Data Exchange Server, and an Access Gateway. The Data Exchange Server connects to the organization's anti-malware solution
- **Lan tier** - includes an Access Controller and Data Exchange Server. The Data Exchange Server connects to the organization's: business applications, file storages (e.g. NTFS), EFFS/MFT solutions, Email server, identity services (e.g. Active Directory), data leak prevention (DLP) solutions, etc.

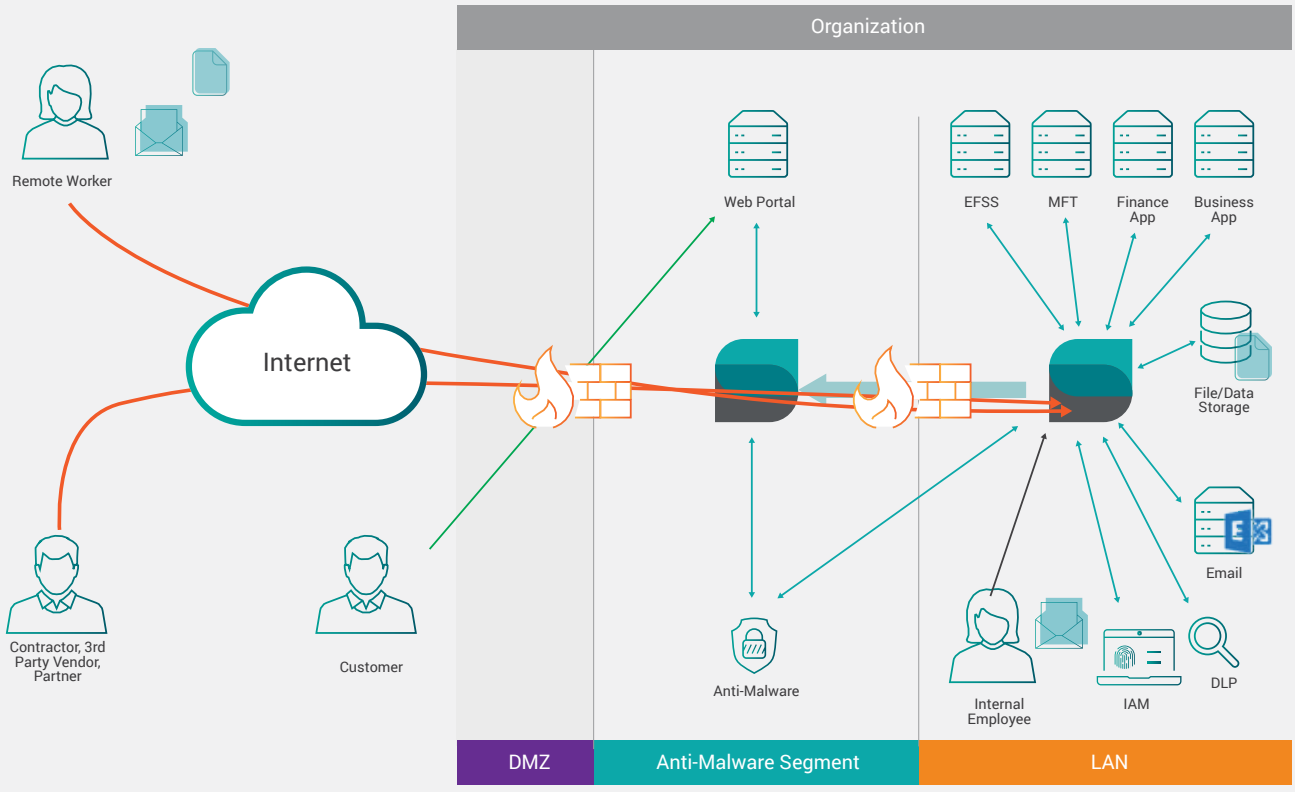

Figure 1 - Safe-T Secure File and Email Access

Components Functions

Each component within the solution has its own function:

- The Access Gateway located in the DMZ segment and the Access Controller located in the Anti-Malware segment, protect the Data Exchange Server located in the Anti-Malware segment.
- The Data Exchange Server located in the Anti-Malware segment is responsible for passing any incoming file or safe-reply from the outside world to the anti-malware solution.
- The Access Gateway located in the Anti-Malware segment and the Access Controller located in the LAN segment, protect the Data Exchange Server located in the LAN segment.
- The Data Exchange Server located in the LAN segment is responsible for controlling and securing all outgoing secure emails and file transfers, as well as any access to locally and cloud stored files.

Secure File and Email Access Use Cases

Secure Access to NTFS folders - SmarTransferTM SIFS allows internal and external users to gain transparent access to secure storages over HTTP/S rather than SMB.
What appears as a standard mapped network drive is, in reality, a secure, encrypted and access-controlled channel to interact with files – upload, download, copy, open, delete, etc. - while not relying on vulnerable protocols such as SMB.
All transactions are subject to Safe-T's SecureStream policy and workflow engine, thereby ensuring secure and controlled access to any file type and content meeting governance and audit requirements.

Secure Email - Safe-T empowers organizations to securely provide any user, access to sensitive files and data, via a secure email.
Secure emails can be sent from users or applications to any user, application, or device, without disrupting the normal routine by not requiring the recipient to install software or exchange cryptographic keys.
Safe-T Secure Email is seamlessly integrated with Outlook, OWA, Gmail, or deployed in the network behind the scenes.
Business users can send secured emails with attachments of any size and type to registered or ad-hoc recipients, providing a simple, easy to use, and fully auditable alternative to PGP.
Recipients can even reply securely, to ensure end-to-end security for the entire email conversation.

Employee Collaboration - Safe-T can be deployed as a robust and secure enterprise file sync and share (EFSS) solution, enabling business users to securely access, collaborate and share data with business functions, business users, and business partners across the globe. Access to data can be done without the need for a VPN.

Safe-T is comprised of multiple secure folders (Secure Virtual Vaults), 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 be either a local folder, network folders, applications, cloud storage, etc.
Access to the Secure Virtual Vaults and sharing of files with other users, is based on user credentials and can be done via a variety of client interfaces all providing the same unified look and feel:

- User-friendly Outlook plug-in
- Web user interface
- SmarTransfer® native access
- Mobile application for iOS and Android

SFTP Replacement – Safe-T allows organizations to replace legacy S/FTP deployments, by integrating seamlessly with business applications, legacy systems and proprietary tools. Safe-T adds security layers to existing S/FTP deployments, including workflows, policy enforcement, integration to non-SFTP storages, authentication, data scanning and data encryption.
Safe-T can operate as both a S/FTP server and S/FTP client. For example, this unique capability allows receiving files uploaded from a SFTP client and storing them secured in a NTFS folder.

Capabilities

Deploying Software Defined Access for secure File and Email Access provides the following capabilities:

- Firewall is constantly in deny-all state, no open ports required for access
- Secures file access and exchange scenarios in one platform
- Controls, manages, and transfers files and data from any source to any destination
- Deployed on-premise or in the cloud
- Stores all files secured and encrypted
- Supports human and application file access and exchange scenarios
- Highly scalable solution
- SecureStreamTM policy and workflow engine
- Dozens of pre-built Safe-T Connectors to business applications, security solutions, data repositories and cloud services
- Full access control and policy enforcement on any file stored or manipulated
- Full auditing of all “where, what, who, and when” file access and exchange
- Highly intuitive and simple end user interfaces
- Client-less, online editing of documents
- Remove the need for VPN access

Benefits

The benefits of providing application access via Safe-T's Secure File and Email Access:

- **Comply with policies and regulations (GDPR, HIPAA, etc.)**
- **Reduce operational and capital costs through consolidation**
- **Hide files from unauthorized users**
- **Prevent file exfiltration, leakage, malware, and ransomware**
- **Client-less file access**
- **Control usage of files**
- **Consolidate all Human and application file access scenarios in one platform**
- **End-to-end monitoring of file access flow**

Feature List

Access Component

Feature	*Comments*
System Level Features	
High availability (HA) Ability to perform high availability/clustering mode in the same data center and between data centers	Safe-T Secure Application Access solution can be setup in HA using an external load balancer or application delivery controller. In addition, a single Access Controller can operate with multiple Access Gateways and Authentication Gateways.

Feature List

Access Component

Feature	Comments
System Level Features	
Disaster recovery Ability to failover to another data center in the event of application unavailability or site disasters	Safe-T Secure Application Access solution can be setup in a disaster recovery architecture using an external load balancer or application delivery controller
Deployment	On-premises or Hybrid-cloud
Access Features	
Patented Reverse-Access technology	Safe-T's reverse-access technology is patent protected. The Reverse-access technology is a dual node technology, which removes the need to open any ports within a firewall, while allowing secured application access between networks (through the firewall)
Requires opening firewall ports	No
Support any TCP based application / service	Safe-T Secure Application Access solution supports any TCP based application / service, applying reverse-access to it
Logical Network Segmentation	Logically segment the network, deploying a Zero Trust model, to reduce the risk of cyber-attacks from reaching internal network segments, or laterally moving throughout your network
HTTPS Proxy	Safe-T Secure Application Access solution supports HTTP/S based applications / services
WebDAV Support	Safe-T Secure Application Access solution supports WebDAV based file access

Feature List

Access Component

Feature	Comments
Access Features	
SSL Off-loading	Safe-T Secure Application Access solution support terminating SSL client connections destined to an application / service
Multi-factor authentication	Safe-T Secure Application Access solution supports authenticating and authorizing users with multi-factor identity management tools before service requests to back-end applications can take place. • Authentication via the organization's LDAP or Active Directory systems, • Authentication using OTP as 2nd factor for NTLM or Kerberos • Integration with 3rd party authentication solutions • NoPost authentication based on emails • SSO support
Client-less and VPN-less application access	Safe-T Secure Application Access solution does not require any client application to be installed on the end-user's machine
Per User Group Access Policies	Yes
Time/Date Based Access Policies	Yes
Management and Operation	
Using a Web for full management	Yes
System logs	Yes
External Provisioning	Yes, via TCP API for reverse-access rules

Feature List

Data Exchange Component

Feature	Comments
System Level Features	
Server base platform to host the server application	– VM/Hardware – Windows Server
Client base platform to run the client application	– VM/Hardware – Windows Server
64-bit Application Support	Safe-T products are 64-bit compatible – Microsoft Exchange Server add-on (SMTP Listener) – Outlook Plug-in (for MS Office 2003/2007/2010/2013/2016) – SmarTransfer – Web UI – Automation Utilities
High availability **Ability to perform high availability/clustering mode in the same data center and between data centers**	Safe-T Data Exchange Server connects to a remote SQL DB server and can provide storage over the LAN, administrators can have more than one Safe-T Data Exchange Server installed on the premises to provide DR capabilities
Disaster recovery **Ability to failover to another data center in the event of application unavailability or site disasters**	Safe-T Data Exchange Server connects to a remote SQL DB server and can provide storage over the LAN, administrators can have more than one Safe-T Data Exchange Server installed on the premises to provide DR capabilities
Users database **Location where user information is stored**	Safe-T Data Exchange Server uses an SQL database
Configuration database **Location where configuration settings are stored**	Safe-T Data Exchange Server uses an SQL database. Safe-T supports multiple protocols including NTFS/NFS, thus allowing customer to work directly with existing data centers
Database Encryption of sensitive information inside local SQL/MySQL database with which MFT product works.	All sensitive information is encrypted including contacts, passwords, emails, packages, messages, etc. Encryption is done using AES 256-bit.

Feature List

Data Exchange Component

Feature	Comments
System Level Features	
Full Web access interface for internal/external users and guests	Yes
Ease of Use	
Ability to use Secure File Transfer using standard mail client (Outlook)	Yes, using Safe-T's unique Outlook plug-in
Installation file for Outlook plug-in	Single or centralized deployment using SMS/ GPO
Installation file for Outlook plug-in	Single or centralized deployment using SMS/ GPO
Using the "Send To ..." feature with mouse right-click to send secure emails	Yes
Power user options **Ability to set advanced options onto attachment/ outgoing messages displayed in composing new email**	Safe-T allows the administrator to predetermine advanced options for the users or allow them to use the options before sending the package. In addition, Safe-T provides power users with advanced options, including: – File expiry – Body encryption – Max downloads – Safe Reply – OTP – Password
Methods of attaching an attachment to an Email	Two options: 1. As a Link 2. As a secure PDF
Ease of accessing attachments for internal users	– Receive a URL for the file located on the Safe-T Data Exchange Server or over the network. – Internal users can download the file onto their desktop or open the file directly by using the UNC URL path.

Feature List

Data Exchange Component

Feature	Comments
Ease of Use	
Ease of accessing attachments for external users (recipients)	– Do not need to install any software, pre-register, or even be notified prior to the file transfer process (ad-hoc users) – Ability to allow users to download with/without login – External returning user with local user name and password is supported
Detailed attachment and transaction tracking (who, when, what?)	Any user or application which touches the package/attachment is tracked Tracking is done using a dedicated log within Outlook
Ability to invite recipients to upload files without agent	Yes, using Safe-Reply - External recipient receives a link for safe reply of files with expiration
Secure Data Exchange Scenarios	
Human Data Exchange	• Secure Email • S/FTP • Consumer Cloud storage • Human-Based File Upload • Employee Collaboration • NTFS access over WebDav
Application Data Exchange	• Business to Business Data Exchange • Application to Application Data Exchange • Application-Based File Upload
Secure Email Features	
Ability to send file or folder	Yes, local or network directories
Ability to designate directories for automatically sending of files from different application	Yes (command line and automated flow)

Feature List

Data Exchange Component

Feature	Comments
Secure Email Features	
Splitting large files/directories	Yes
Sync with Outlook phonebooks	Yes
Ability to distribute to users' PCs through Microsoft SCCM (System Center Configuration Manager)	Yes
Control extension file type	Any type. You can control which files type of files are allowed or blocked
Communication protocol(s) between Safe-T Data Exchange Server and Data Storage	– HTTP/S – WebDAV – FTP – SFTP – SQL – REST API – etc.
Ability to perform applied policy scanning on an outgoing attachment	Yes
Ability to perform applied policy scanning on an incoming attachment	Yes
Ability to enforce policy on any file type or size	Yes
Ability to expire attachments	Yes – by download times – by date/hours/minutes
Ability to compress attachments (file, folder)	– Zip – RAR – AES – etc.
Ability to encrypt the attachment	Yes, AES 256 or any other type of external encryption

Feature List

Data Exchange Component

Feature	Comments
Secure Email Features	
Safe Spaces are visible in Outlook when plug-in is installed	Yes
Ability to resume uploads when network connection is available	Yes
Ability to allow external recipients to register for first time login to Safe-T	Yes
Ability to allow external recipients to access Safe-T Data Exchange Server via web access	Yes
Body encryption for secure messaging	Yes
Ability to allow or block specific users from sending messages to specific recipients	Yes, using built-in Message Delivery Restrictions management
Ability to restrict so that only intended recipients can download the attachments	Yes, done by combining security methods: 1. OTP via Text Message [SMS] 2. Limit max downloads 3. Create a short expiry time for sent messages (few hours)
Ability to archive email together with original attachment	Yes, supports archiving solutions: – Symantec Enterprise Vault – CommVault Archiving
Ability to scan attached/uploaded data	Yes, using internal DLP or external 3rd party DLP solutions
Ability to inform the sender using Outlook about files which were downloaded	Auto email notification when recipient(s) downloads files
OTP via mobile or SMS on email	Yes
File encryption at rest	Yes

Feature List

Data Exchange Component

Feature	Comments
Secure Email Features	
File encryption in transit	Yes, using PDF encryption
HTTPS secured connection	Yes
Ability to sign files with certificates	Yes, and as SDK
Data manipulation (external tools)	Yes
X509	Yes
S/MIME support	Yes
Ability to replace the sent package after sending the email	Yes
Secure Email Features	
Via Safe-T mobile app	Yes
Via Safe-T web portal	Yes
Workflow auditing and logging	Yes
Integration with Storages	Yes
Secure File Access	
NTFS file access over HTTPS	Yes
Control file access	• Supports file I/O operations on remote file servers with full file function capabilities, such as: Upload, download, copy, create, open, move, delete and NTFS complimentary permissions associated with users and groups.

Feature List

Data Exchange Component

Feature	Comments
Secure File Access	
Control file access	• Clientless capabilities minimize the complexity of managing desktop client installations and upgrades, and it is transparent to operating systems (Windows/Mac/Linux). • Support using HTTP URL only and authenticating using standard authentication methods: Kerberos/ Negotiate/NTLM/Multi-factor/IDP/ Header-Auth/AUTH2/Smart-Cards/etc. • Server-side capabilities maximize the security of overall user file transmissions. • Ensures secure and controlled access to any file types and content. • Acts as a secure file gateway between users and remote file servers while enabling third-party integration and enforced policies (AV/DLP/etc.). This helps to prevent any unauthorized access or usage (such as changing file original format, encrypting files, Ransomware attacks, etc.). • From the user's perspective, it acts as any mapped drive, including sharing links to the mapped drive with other users.
Management and Operation	
LDAP integration **Ability to manage users via Active Directory**	Yes
Ability to manage passwords of Active Directory and non- Active Directory users	Yes, using Active Directory policy and built-in password management policy for non-Active Directory users
Ability to self- manage inactive users	Yes
Using a Web admin for full management	Yes

Feature List

Data Exchange Component

Feature	Comments
Management and Operation	
Storage management of occupied space of uploaded files with the ability for easy delete	Available (Disk Quota Management)
File archiving	Yes
Users/group control integrated through Active Directory	Yes
Schedule management jobs Active Directory Sync, Cleaning up the System, reports	Yes
Ability to manage and limit file and disk size and enforce volume quota per user	Yes
Report generation	Yes, detailed, simple, summary, etc.
Ability to schedule the generation of reports	The following reports can be scheduled for generation (manually or via SDK): – Generate report when an email is sent/ received – manager and user level – Generate report detailing the total sent/ received files and sizes – manager and user level – Safe-T allows generating manager and user level reports
Auditing - ability to track all email attachments records and administrative changes	Yes
Policy on group and individual users	Yes
Policy regards file types allowed/not allowed	Yes

Feature List

Data Exchange Component

Feature	Comments
Management and Operation	
External Provisioning	Yes, via REST API
Safe-T Connectors	
Protocols	Yes
Active Directory	Yes
WebDAV	Yes
HTTP/S based applications	Yes
NAS	Yes
NTFS	Yes
SFTP	Yes
SMTP	Yes
SOAP/WSDL	Yes
SSH	Yes
SQL	Yes
Applications	
Enterprise Applications	– Oracle – SAP – IBM AS400 – SharePoint

Feature List

Data Exchange Component

Feature	Comments
Safe-T Connectors	
Antivirus and Sanitization solution integration	– Check Point Sand Blast – AVG (Client/Server) Server – Gate Scanner – RE-SEC – OPSWAT – ODI – McAfee – Symantec SEP – Trend Micro OfficeScan – WinClam – SDK
Consumer Cloud Storage	– Box – DropBox – OneDrive – Google Drive
DLP integration	– Symantec – WebSense – McAfee – SDK
PDF Encryption	Yes
PDF Sign	Yes