PRODUCT BRIEF

SECURE FILE ACCESS

safe-t
Masters of Access

Contents

Introduction 3

The Safe-T Solution 3

How It Works 4

Capabilities 5

Benefits 5

Feature List 6

Introduction

Sensitive data leakage by internal employees is a major concern for any organization in terms of data protection, but for highly secure organizations such as defense contractors, military manufacturers, intelligence agencies, law enforcement agencies, etc, it is the most pressing concern and may affect the organization in many ways including jeopardizing human lives.

Such organizations are usually cut off from the outside world, but they hold the most highly sensitive data in the world, so the threat is internal rather than external. The internal threat can be any of the following – employees, 3rd party contractor working within the facility, or the IT administrator managing the file storages.

The problem is that like their enterprise counterparts, also highly secure organizations use file shares in order to provide users with access to organization data, as well as ensuring data is regularly backed up.

While providing ease of access to files, standard files shares do not provide high levels of access and usage controls, but rather basic user permissions. In addition, the main protocol used for file shares is Server Message Block (SMB) also known as Common Internet File System (CIFS).

But while SMB has become in the center of all organizations, it's inherent vulnerabilities have been exploited as part of various attacks. The continued use of the SMB protocol is a major security concern for organizations globally, regardless their type.

The Safe-T Solution

Safe-T's Secure File Access (SFA), allows internal users to gain transparent access to secure storages over the standard HTTP/S protocol.

What appears as a standard mapped network drive is actually a secure, encrypted and access-controlled channel exposing sensitive information/files with the right authorization rights to upload, download, copy, open, delete, view, etc all according to "need to know basis" and permissions, while not relying on the vulnerable SMB protocol.

All transactions are subject to Safe-T's policy and workflow engine, thereby ensuring secure and controlled access to any file type file content, meeting governance and audit requirements.

Safe-T's Secure File Access integrates with the organization's authentication solution (e.g. Active Directory), transparently authenticating the user when they open their mapped drive. The list of presented Safe Spaces (folders) displayed to the user, depends on the user's group and permissions.

How it Works

Safe-T's Secure File Access can be deployed in one of two deployment scenarios:

Single Segment

As can be seen in figure 1 below, when deployed in a single segment, the solution requires a single SFA unit which is connected to the organization's file server, and authentication tier (e.g, Active Directory).

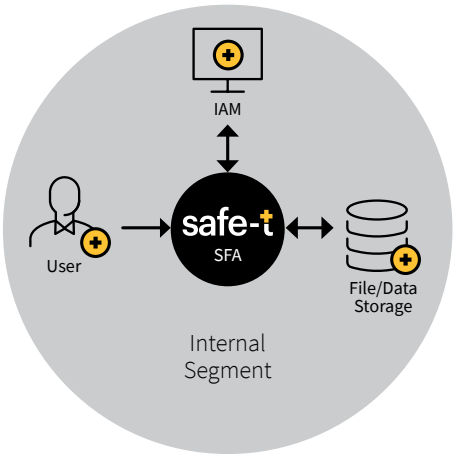


***Figure 1** - Safe-T Secure File Access – Single Segment*

Multiple Segments

As can be seen in figure 2 below, the solution is composed of multiple components. The solution is usually deployed in one or more internal segments within the organization.

- **Internal Segment 1** – includes a Safe-T SFA which is connected to the organization's file server, and authentication tier (e.g, Active Directory). If users connect to this segment for other segments, then an Access Controller is deployed also in Internal Segment 1. The Access controller communicates with an Access Gateway in other internal segments.
- **Internal Segment 2** – includes an Access Gateway which communicates with the Access Controller in Internal Segment 1. It is used to allow users from Internal Segment 2 to reach the Safe-T SFA server without the need to open the firewall between the two segments.

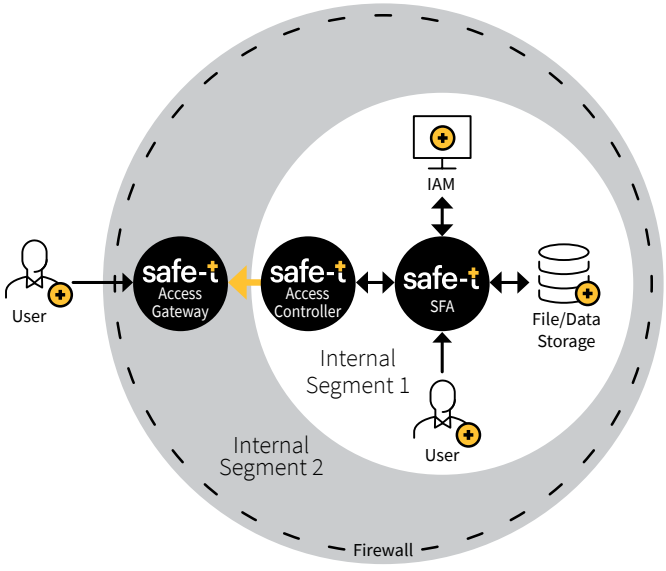


***Figure 2** - Safe-T Secure File Access – Multi Segment*

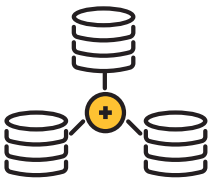
Capabilities

Deploying Safe-T's Secure File Access provides the following capabilities:

- Deployed as a virtual machine, seamlessly integrates into existing file shares
- Server-side capabilities maximize the security on overall users file transmissions
- Zero SMB protocol usage, connection using HTTP/S protocol from client to Safe-T
- As opposed to other solutions, Safe-T SFA is clientless and does not require any installation on the user desktop. Clientless deployment minimizes the complexity of managing desktop client installations and upgrades, and it is transparent to any operating systems
- Access and permissions control ensures secure and controlled access to any file types and content
- Supports file operations with full file function capabilities, such as: Upload, download, copy, create, open, move, delete
- Prevents any unauthorized file access or usage - changing file original format, encrypting files, etc
- Built-in file encryption
- Full audit trail and reporting to SIEM solutions (e.g. Arcsight)
- View only options, without the option to download the sensitive information to the local work station

Benefits

Full segregation of duties between IT administrators and business users

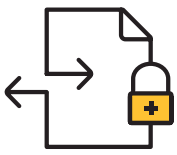


Seamless integration into existing file access environments

Simple and easy deployment

Reduce the risk of data theft, and data leakage attacks

Reduce the overall network attack footprint by removing SMB protocols



Access Control ensures secure and controlled access to any file types and content

Ability to interact with organization security and data protection tools

Brings back the control over sensitive information from the users to the organizations

Features List

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 File Access solution can be setup in HA using an external load balancer or application delivery controller.
Disaster recovery Ability to failover to another data center in the event of application unavailability or site disasters	Safe-T Secure File Access solution can be setup in a disaster recovery architecture using an external load balancer or application delivery controller
Deployment	On-premises
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
WebDAV Support	Safe-T Secure File Access solution supports WebDAV based file access
Client-less access	Safe-T Secure File Access solution does not require any client application to be installed on the end-user's machine
Management and Operation	
Support a management interface	Yes
System logs	Yes
External Provisioning	Yes, via TCP API for reverse-access rules
System Level Features	
Server base platform to host the server application	VM
Client base platform to run the client application	• VM/Hardware • Windows Server
Configuration database *Location where configuration settings are stored*	Safe-T Secure File Access uses an SQL database.

Features List

Feature	Comments
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.
Ease of Use	
Detailed attachment and transaction tracking (who, when, what?)	Any user or application which touches a file is tracked
Communication protocol(s) between Safe-T Secure File Access and Data Storage	SMB
Communication protocol(s) between user and Safe-T Secure File Access	WebDAV (HTTPS)
Ability to enforce policy on any file type or size	Yes
File encryption at rest	Yes
HTTPS secured connection	Yes
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. • 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/ Header-Auth/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. 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.

Features List

Feature	Comments
Management and Operation	
LDAP integration *Ability to manage users via Active Directory*	Yes
Users/group control integrated through Active Directory	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 detailing the total sent/received files and sizes – manager and user level • Safe-T allows generating manager and user level reports
Policy on group and individual users	Yes
Policy regards file types allowed/not allowed	Yes
Protocols	
Active Directory	Yes
WebDAV	Yes
HTTP/S	Yes
NTFS	Yes