PRODUCT BRIEF

# SECURE FILE ACCESS

Version 2 | 二版
www.version-2.com

safe-t
Masters of Access

# Contents

# Introduction

Data leakage is caused by employees is a major concern for any organization. But for highly sensitive organizations such as hospitals and government agencies, it is a critical concern that may impact the organization in many ways, and in some cases, may even put lives in danger.

The problem is that most organizations use standard file shares to provide users with access to organizational data, as well as to ensure data is regularly backed up. While they provide ease of access to files, standard file share like SMB do not provide high levels of access and usage controls, but rather, they use basic user permissions, so there's no way to enforce strong authorization and segregation of duties. If an employee, contractor, or IT admin with malicious intent gets access to files they should not be able to view, it could spell disaster. The epic Snowden incident proved that SMB threats are not only entirely possible, they are probable-that is, if the proper precautions are not taken.

## The Safe-T Solution

Safe-T® Secure File Access (SFA), part of our Zero Trust set of solutions, allows users to obtain transparent access to organization's distributed SMB file shares, without exposing direct SMB communication protocol.

SFA leverages the existing infrastructure, transforming your standard network drive to a Zero Trust, access-controlled drive, exposing sensitive information on a "need to know basis" only, while eliminating the need to rely on insecure file permissions and vulnerable distributed SMB protocols.

With SFA, you can "Zero Trust" your files to create a truly comprehensive security strategy.


**Hong Kong**
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

**Taiwan**
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

**Singapore**
Tel : (65) 6296 4268
Email : sales@version-2.com.sg

# How it Works

SFA acts as a Distributed File System Proxy for Microsoft Windows SMB servers. By using any Client Desktop typically built-in under all Operating Systems (Windows, Mac, etc), users can natively configure drive mapping under their OS. SFA removes the need of group membership and the corresponding permissions so that NTFS and ACL are inherited and reflected to the users.
Safe-T's Secure File Access can be deployed in one of two deployment scenarios:

## Standalone

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

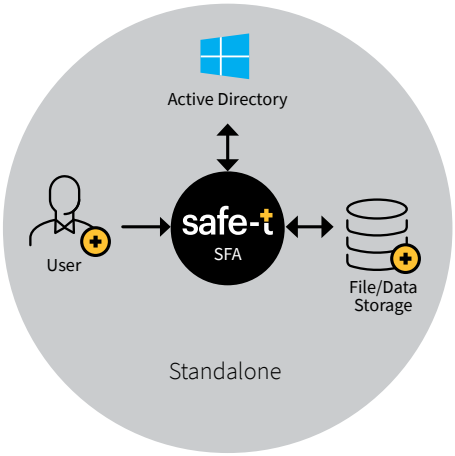



Figure 1 - Safe-T Secure File Access – Standalone

## Perimeter Access

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.

- **Perimeter Access 1** – includes a Safe-T SFA which is connected to the organization's distributed SMB servers storage, and authentication tier (e.g, Active Directory). If users connect to this segment for other segments, then an Access Controller is deployed in Perimeter Access 1 as well.
- **Perimeter Access 2** – includes an Access Gateway which communicates with the Access Controller in Perimeter Access 1. It is used to allow users from Internal Perimeter Access 2 to reach the Safe-T Secure File Access server without the need to open the firewall between the two segments.

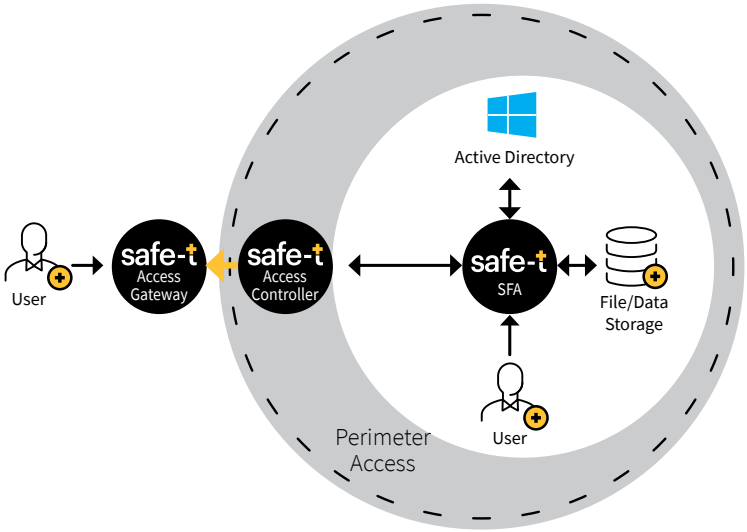



Figure 2 - Safe-T Secure File Access – Perimeter Access


**Hong Kong**
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

**Taiwan**
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

**Singapore**
Tel : (65) 6296 4268
Email : sales@version-2.com.sg

# Capabilities

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

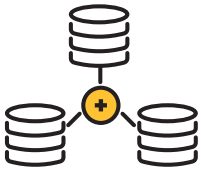
- Deployed as a virtual machine.
- Acts as a secure HTTP file proxy between users and remote file servers.
- Transparent and secure access to sensitive information over the standard HTTP/S protocol.
- Integration with your organization's Active Directory authentication service.
- Full support of Windows Access Based Enumeration – only directories the user has access to, will be shown.
- High availability support - Active-Active/ Passive
- Supports disaster recovery architecture scenarios
- One-click rollback solution
- Removes SMB protocol from client segment connection using HTTP/S protocol from client to Safe-T
- Clientless deployment minimizes the complexity of managing desktop client installations and upgrades
  - Cross platform support
  - Compatible with GPO/ SSCM distribution
- True Type engine to ensures secure and controlled access to various file types and content
- Prevents any unauthorized file access or usage, validate on every uses action (request → validate → approved)
- Full audit trail and reporting of user and admin activities
- Fully integrated with Safe-T SAA solution

# Benefits

## The benefits of application access via Safe-T's Secure File Access:

**Full segregation of duties**

Isolate IT from business users



**Seamless Integration**

Hassle-free unification with current file storage solutions

**Returns control over sensitive information**

Keep your data in the right hands

**Simple and easy deployment**

No client installation

**Enhanced risk reduction**

Reduce Risk of data theft and leakage

**Reduces the likelihood of ransomware attacks**

By removing the insecure SMB protocol

**Prevent any unauthorized access or usage**

changing file original format, encrypting files, Ransomware attacks, etc



**Hong Kong**
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

**Taiwan**
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

**Singapore**
Tel : (65) 6296 4268
Email : sales@version-2.com.sg

# Features List

| Feature | Comments |
|---|---|
| **System Level Features** | |
| High availability (HA)<br>Ability to perform high availability/clustering mode in the same data center and between data centers | Safe-T's Secure File Access solution can be set up in HA using an external load balancer or application delivery controller |
| Disaster recovery<br>Ability to failover to another data center in the event of application unavailability or site disasters | Safe-T's Secure File Access solution can be set up 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 |
| HTTP/S Support | Safe-T's Secure Application Access solution supports HTTP/S based file access |
| Clientless access | Safe-T's Secure File Access solution does not require any client application to be installed on the end-user's machine |
| **Management and Operation** | |
| Supports management interface | Yes |
| System logs | Yes |
| **System Level Features** | |
| Server base platform to host the server application | VMware vSphere, Microsoft Hyper-V |
| **Ease of Use** | |
| Detailed attachment and transaction tracking (who, when, what?) | Reports about each usage made in Secure File Access |
| Communication protocol(s) between Safe-T Secure File Access and Data Storage | SMB V1,2,3 |
| Communication protocol(s) between user and Safe-T Secure File Access | HTTPS/S |
| HTTPS secured connection | Yes |
| NTFS file access over HTTPS | Yes |

# Features List

| Feature | Comments |
|---|---|
| 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 permissions associated with users and groups.<br>• Clientless capabilities minimize the complexity of managing desktop client installations and upgrades, and it is transparent to operating systems (Windows/Mac/Linux).<br>• Server-side capabilities maximize the security of overall user file transmissions.<br>• Ensures secure and controlled access to any file types and content.<br>• 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).<br>• 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 (Active Directory) | Yes |
| Users/group control integrated through Active Directory | Yes |
| Report generation | Yes, detailed, simple, summary, etc. |
| Policy regarding file types allowed/not allowed | Yes |
| **Protocols** | |
| Active Directory | Yes |
| SMB | Yes |
| HTTP/S | Yes |
| NTFS | Yes |