safe-t

focality

Safe-T ZoneZero® SFA

The first ever centralized MFA solution for SMB Distributed File Shares

Safe-T's ZoneZero SFA solution is the first ever centralized solution designed to act as an SMB proxy, converting HTTP/s traffic to SMB, removing the need to open SMB connection for end-user clients. In addition, it offers the ability to add multi factor authentication (MFA) for users accessing any SMB based file share. And most importantly ZoneZero SFA is fully transparent to end-users and does not impact performance.

Most files today are internally accessed using SMB (Server Message Block) protocols. SMB is the standard in file access across almost all verticals—from manufacturing to financial institutions to healthcare and governments. In the mid-1990s Microsoft used SMB 1.0 in its LAN Manager and renamed the protocol CIFs. Subsequently, Microsoft released SMB versions 2.0/3.x which are used in Windows 10 and Windows Server 2019[1]. The files are stored in file servers, and the end user can access them with ease and gets a convenient, effortless file usage experience. It's a process that we tend to take for granted, even though a whole lot of complex processing is taking place behind the scenes.

But for all its utility, SMB comes with some inherent security vulnerabilities. Both WannaCry and NotPetya, two devastating ransomware variants that wreaked total havoc on organizations worldwide in 2017, spread as quickly as they did thanks to a vulnerability in the SMBv1 protocol. That Microsoft recommends disabling SMBv1 is old news. But in the wake of WannaCry and NotPetya, experts began calling for the disabling of versions 2 and 3 as well, fearing these versions may have been compromised as well.

And their fears proved correct; in the past few years, there have been numerous buffer overflow proofs-of-concept in which SMBv2 and SMBv3 have been compromised to send out malicious links to users and create DoS exploits.

Just what are some of the security failings associated with SMB versions 2 and 3?

- SMB communication protocol is required between endpoint devices and distributed SMB file shares
- No access controls are provided
- Anyone one can steal/access files
- It's not encrypted
- Users can still see files after use

If you were hoping these newer versions would be able to prevent leakage, sadly, that's not the case.

Lack of strong access control

The problem is most organizaions use SMB file shares to provide their users with access to data, as well as to ensure data is regularly backed up. Although end users may have easy access to files, standard file share protocols like SMB are unable to provide high levels of access control, for example strong authentication and usage controls. Instead, they use basic user permissions, so there is 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. Think about the large number of users who access files from different devices and end-points, and from different locations, the ability of standard files shares to verify user identity, and control access to sensitive resources becomes a huge challenge.

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.

Introducing Safe-T ZoneZero Secure File Access (SFA)

Safe-T® ZoneZero Secure File Access (SFA) is the simple and smart way to provide employees and customers secure access to corporate distributed SMB file shares, without exposing the direct SMB communication protocol on Port 445 to endpoint devices.

ZoneZero SFA leverages existing infrastructure and provides endpoint devices with secure HTTP/S-based communication only, to corporate networks.

With ZoneZero SFA, organizations can **transform any** distributed SMB Servers **into a Zero Trust, access-controlled secure file access service, exposing sensitive information on a "need to know basis" only,** while eliminating direct access to corporate distributed SMB Servers and networks.

To provide secure access to distributed SMB servers storage using HTTP/S Protocol only, SFA acts as a Distributed File System Proxy for Microsoft Windows SMB servers.

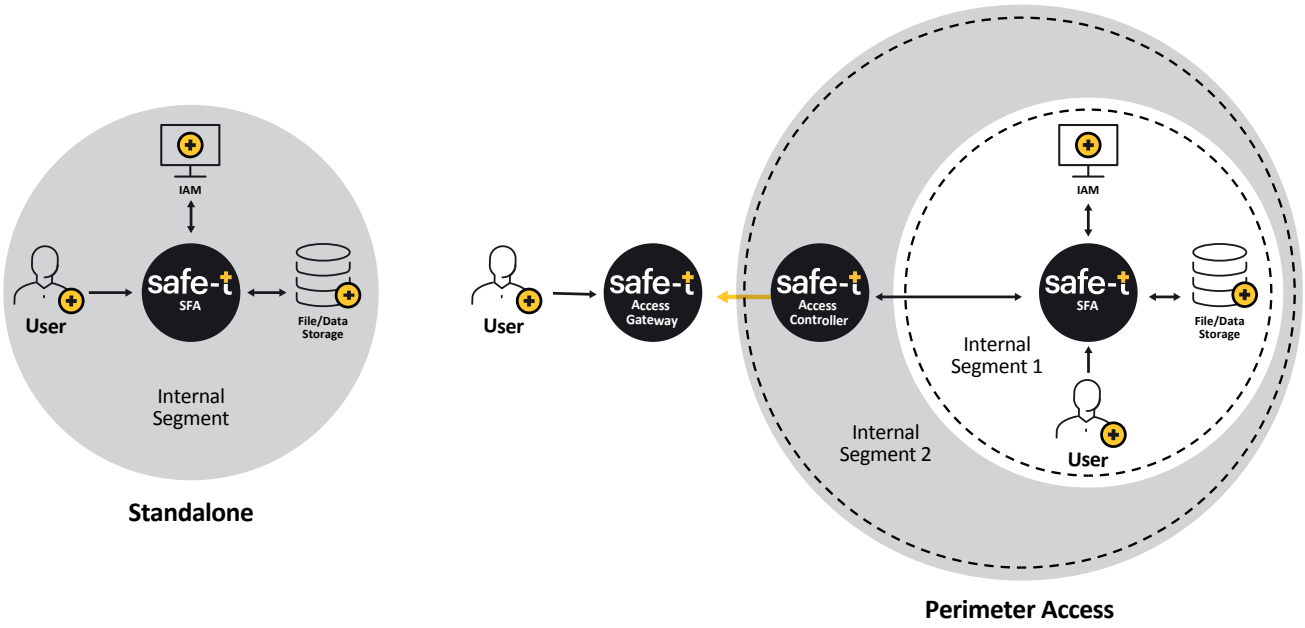
Using any WebDAV client typically built-in under all Operating Systems (Windows, Mac, etc), or Safe-T's ZoneZero SFA client application, employees and customers can natively configure Drive Mapping under their OS.

ZoneZero SFA learns group memberships and the corresponding permissions, so that NTFS and ACL are enforced and reflected to endpoint users.

Using ZoneZero SFA, it is now simple to add advanced authentication options to SMB file share access. Rather than relying only on Active Directory authentication, SFA integrates with any authentication and MFA tool (ADFS, OIDC, biometric, REST based, etc) and acts as a centralized authentication control point for any user accessing a file share.

Safe-T ZoneZero SFA uses an innovative approach of combining MFA and Zero Trust File Access policies to control authentication and access across all enterprise files shares which are generally regarded as MFA-unsupported. This is done without requiring any changes to file shares, or development of custom code.

Imagine adding fingerprint validation before accessing a file share, now it's possible! Just integrate SFA with your biometric server and SFA will handle the rest.



Core product features

- Acts as a secure HTTP/S file proxy between users and remote file servers
- Prevents any unauthorized access or usage (changing original file format, encrypting files, Ransomware attacks, etc)
- Enables users (internal and external) to gain transparent and secure access to sensitive information over the standard HTTP/S protocol, in place of SMB
- Integrates with your organization's authentication service - Active Directory, ADFS, biometric authentication, OIDC based authentication solutions, REST based authentication solutions
- Adds multi factor authentication (MFA) options for SMB file share access
- Windows Access Based Enumeration is fully supported. SFA will only show the directories the logged-on user has access to, even if the distributed SMB server storage contains more than that

Benefits

- Full segregation of duties – Isolate IT from business users
- Seamless Integration – Hassle-free unification with current file storage solutions
- Strong authentication using a centralized authentication and MFA solution
- 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

51 John F Kennedy Parkway, Short Hills, NJ | 888-304-5010
www.safe-t.com

Users are only able to see and access files according to their specific group and permissions and in conjunction with Safe-T's ZoneZero SDP (Software Defined Perimeter) enables secure access to file shares over HTTP/S for internal and external users, with or without the need for a VPN connection. With SFA you can share the secure map drive all over the world, without any need for 3rd party integrations.

And finally, with ZoneZero SFA, you can eliminate the use of SMB protocols between endpoint devices and file storages, to significantly reduce your chances of dangerous ransomware infection on centralized storages.

With Safe-T's ZoneZero SFA, you can give your employees and contractors access to documents and files they need, without compromising on security.

Safe-T ZoneZero SFA offers the following advantages of standard SMB file shares

Features	ZoneZero SFA (Client)	Microsoft (SMB)
Access to SMB VIA HTTP/S Protocol Only	Yes	No
IDP / ADFS / Support for user login Authentication	Yes	No
Software / Biometric for User Device MFA	Yes	No
MFA Support	Yes – REST API, ADFS, OIDC	No

Features	ZoneZero SFA (Clientless)	Microsoft (SMB)
Access to SMB VIA HTTP/S Protocol Only	Yes	No
IDP / ADFS / Support for user login Authentication	Yes - LDAP	No
Software / Biometric for User Device MFA	No	No
MFA Support	No	No