SECURE FILE ACCESS

Prevent Data Leakage and Ransomware Across Your Files and Transfers

safe-t
Masters of Access

Limitations of Secure Message Block (SMB)

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. Created by IBM in the 1980s, it allows users to share folders and files over networks, as if they were on the local machine. 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 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.

More Files, More Risk?

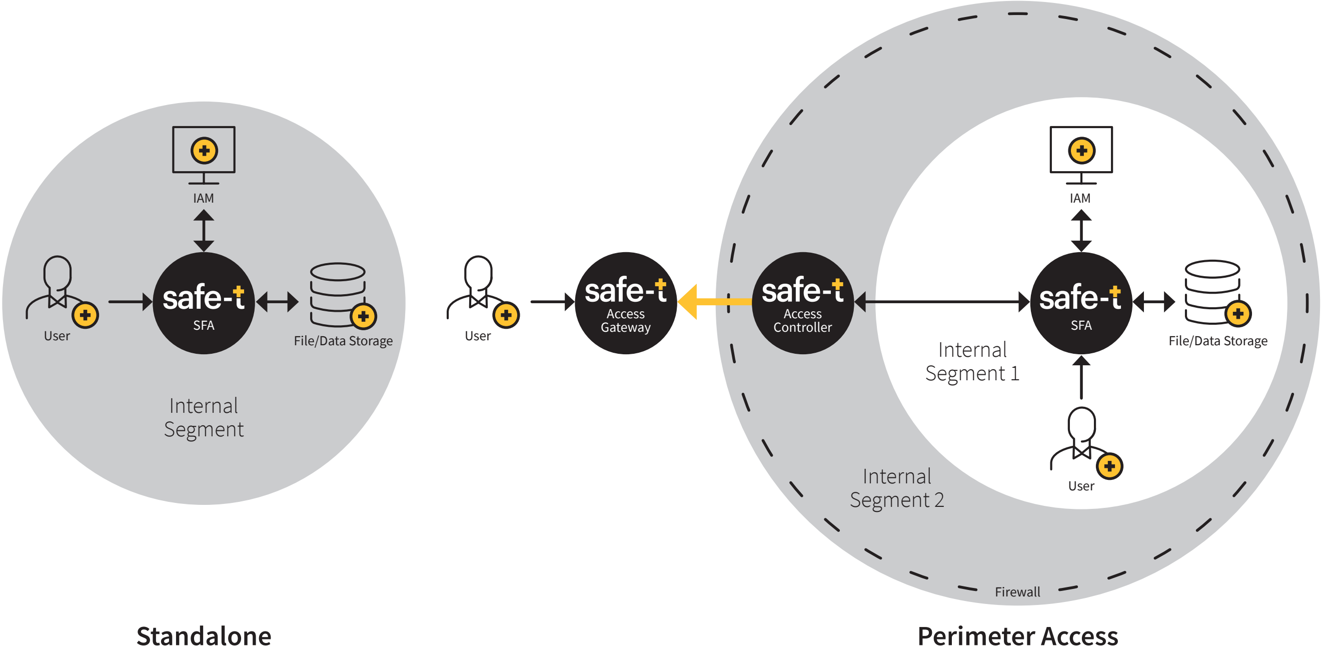
The problem is all organizations use file shares to provide their users with access to data, as well as to ensure that data is regularly backed up. While they do provide ease of access to files, standard file share protocols like SMB are unable to provide high levels of access and usage controls. Instead, 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.

Introducing Safe-T Secure File Access (SFA)

Safe-T® Secure File Access 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.

SFA leverages existing infrastructure and provides endpoint devices with secure HTTP-based communication only, to corporate networks. With 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 HTTPS Protocol only, SFA acts as a Distributed File System Proxy for Microsoft Windows SMB servers. Using any Web Client Desktop typically built-in under all Operating Systems (Windows, Mac, etc), employees and customers can natively configure Drive Mapping under their OS. SFA learns group memberships and the corresponding permissions, so that NTFS and ACL are enforced and reflected to endpoint users.



Core product features:

- Acts as a secure HTTP file gateway 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, and integrates with your organization's Active Directory authentication service.
- 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 of Sensitive Information Access Via Safe-T's SFA Solution:

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

Users are only able to see and access files according to their specific group and permissions and in conjunction with Safe-T's SDP solution, SFA enables secure access to file shares over HTTPS for internal and external users, 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 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 SFA, you can give your employees and contractors access to documents and files they need, without compromising on security.