БЕЗПЕЧНИЙ ДОСТУП ДО ФАЙЛІВ

INTELLIGENT iiTD IT DISTRIBUTION

Запобігання витоку даних та ransomware атакам на ваші файли та при передачі даних

safe-t
Masters of Access

© Copyright 2020 Safe-T Data A.R Ltd.
All Right Reserved.

Обмеження Secure Message Block (SMB) протоколів

Сьогодні доступ до більшості файлів здійснюється за допомогою протоколів **SMB (Server Message Block)**. SMB є стандартом доступу до файлів майже у всіх ітнустріях —від виробництва та фінансових закладів до охорони здоров'я та державних установ. Створений IBM у 1980-х роках, протокол дозволяє користувачам ділитися папками та файлами по мережах так, ніби вони знаходилися на локальній машині. Файли зберігаються на файлових серверах, і кінцевий користувач може легко отримувати доступ до них та користуватися ними в найзручніший спосіб. Це процес, який ми, як правило, сприймаємо як належне, навіть незважаючи на те, що багато складної обробки даних відбувається за лаштунками.

Але при всій своїй корисності, SMB властиві деякі вразливості безпеки. І WannaCry, і NotPetya - два руйнівні варіанти ransomware, які спричинили загальний хаос в організаціях по всьому світу в 2017 році - поширившись досить швидко завдяки вразливості протоколу SMBv1. Те, що Microsoft рекомендує вимкнути SMBv1 – вже не новина. Але на хвилі WannaCry та NotPetya експерти почали закликати також відключити версії 2 та 3, побоюючись, що ці версії також можуть бути скомпрометовані.

І їхні страхи виявилися не безпідставними; за останні кілька років було чимало випадків переповнення буфера, в яких SMBv2 та SMBv3 були піддані компрометації для надсилання шкідливих посилань користувачам та створення DoS експлойтів.

Якими є деякі враздивості безпеки, пов'язані з версіями SMB 2 та 3?	**• Протокол зв'язку SMB необхідний між кінцевими точками та розподіленими спільними файлами SMB** **• Контроль доступу не передбачено** **• Вкрасти / отримати доступ до файлу може кожен** **• Це не зашифровано** **• Користувачі все ще можуть бачити файли після використання**

Якщо ви сподівалися, що новіші версії зможуть запобігти витоку, на жаль, це не так.

Більше файлів, більше ризику?

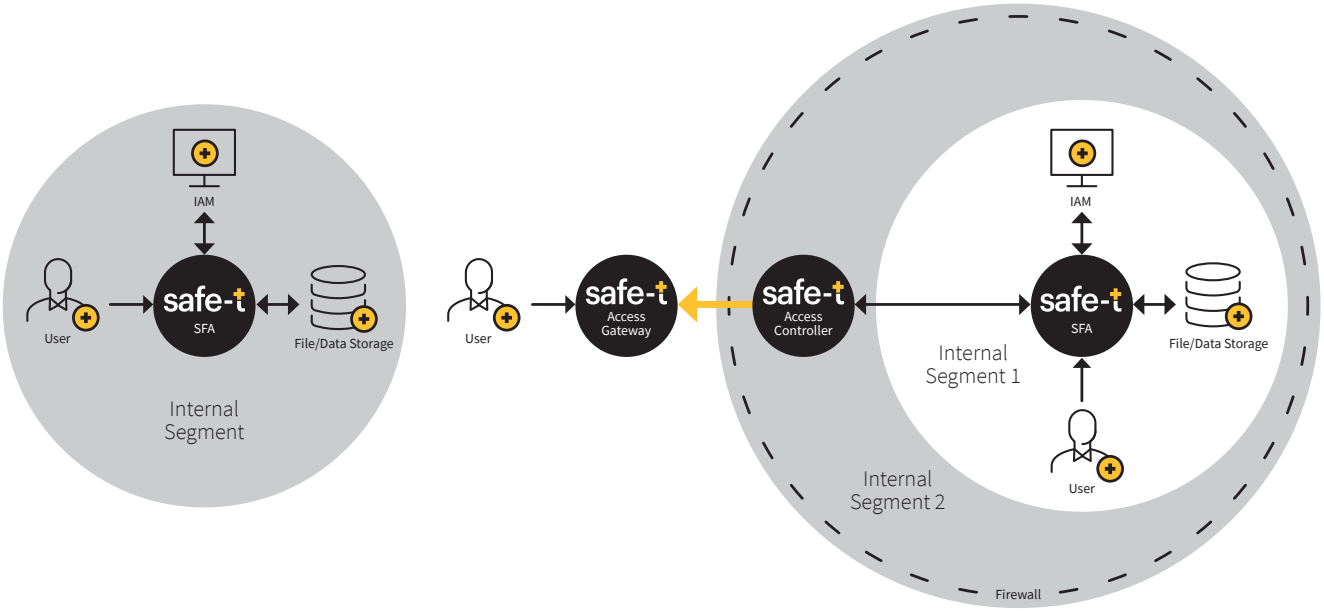
Проблема полягає в тому, що всі організації використовують спільні файли, щоб забезпечити своїм користувачам доступ до даних, а також забезпечити регулярне резервне копіювання даних. Хоча вони забезпечують легкість доступу до файлів, стандартні протоколи обміну файлами, такі як SMB, не можуть забезпечити високий рівень контролю доступу та використання. Натомість вони використовують базові права користувачів, тож немає способу примусово застосувати додаткову авторизацію та розподіл ролей. Якщо працівник, підрядник або IT-адміністратор зі шкідливим наміром отримують доступ до файлів, вони не повинні мати змоги їх переглядати, це може призвести до катастрофи. Епічний інцидент Snowden показав, що загрози SMB не тільки цілком можливі, вони ймовірні - якщо не вжито належних запобіжних заходів.

Представляємо Safe-T Secure File Access (SFA)

Safe-T® Secure File Access - це простий та розумний спосіб забезпечити працівникам та клієнтам безпечний загальний доступ до корпоративних файлів SMB, не встановлюючи прямий зв'язок по протоколу SMB на Порт 445 з кінцевими пристроями.

SFA використовує існуючу інфраструктуру та надає кінцевим точкам безпечний зв'язок з корпоративною мережею на основі лише HTTP. **За допомогою SFA організації можуть перетворити будь-які розподілені сервери SMB в Zero Trust**, безпечний та контрольований сервіс доступу до файлів, надаючи доступ до конфіденційної інформації за принципом "need to know basis ", при цьому виключаючи прямий доступ до корпоративних розподілених SMB-серверів та мереж.

Для надання безпечного доступу до розподілених серверів SMB, використовуючи лише протокол HTTPS, SFA діє як Distributed File System Proxy для SMB-серверів Microsoft Windows. Використовуючи будь-який Web Client Desktop , як правило, вбудований у всі операційні системи (Windows, Mac тощо), працівники та клієнти можуть з самого початку налаштувати Drive Mapping у своїй ОС. SFA вивчає членство в групі та відповідні дозволи, щоб NTFS та ACL були застосовані та відображені для кінцевих користувачів.



Standalone **Perimeter Access**

INTELLIGENT IT DISTRIBUTION

© Copyright 2020 Safe-T Data A.R Ltd. All Right Reserved.

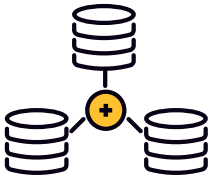
Основні характеристики продукту:

• Діє як захищений шлюз для HTTP файлів між користувачами та віддаленими файловими серверами.
• Запобігає будь-якому несанкціонованому доступу або використанню (зміна оригінального формату файлів, шифрування файлів, Ransomware атаки тощо).
• Дозволяє користувачам (внутрішнім і зовнішнім) отримувати прозорий і безпечний доступ до конфіденційної інформації згідно стандартного протоколу HTTP / S, замість SMB, і інтегрується із службою аутентифікації вашої організації Active Directory.
• Windows Access Based Enumeration повністю підтримується. SFA показує лише каталоги, до яких користувач, що ввійшов у систему, має доступ, навіть якщо розподілене сховище SMB-сервера містить більше, ніж це.

Переваги доступу до конфіденційної інформації за допомогою Safe-T's SFA рішення:

Повна сегрегація ролей

Відокремте IT від бізнес-користувачів

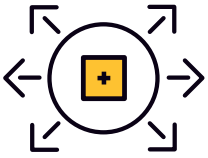


Безшовна інтеграція

Безпроблемне об'єднання з поточними рішеннями для зберігання файлів

Повертає контроль над конфіденційною інформацією

Тримайте свої дані в правильних руках



Просте і легке розгортання

Без інсталяції на стороні клієнта

Дозволяє знизити ризики

Зменшить ризик викрадення та витоку даних

Знижує ймовірність ransomware атак

Видаляючи незахищений протокол SMB

Користувачі можуть бачити та отримувати доступ до файлів лише згідно з їх конкретною групою та дозволами, а спільно із Safe-T's SDP рішенням, SFA надає безпечний доступ до спільних файлів через HTTPS для внутрішніх і зовнішніх користувачів без необхідності підключення до VPN. За допомогою SFA ви можете ділитися secure map drive зі всім світом, не потребуючи сторонніх інтеграцій.

І нарешті, за допомогою SFA ви можете усунути використання протоколів SMB між кінцевими точками та файловими сховищами, щоб значно знизити шанси на зараження небезпечним ransomware на централізованих сховищах.

За допомогою SFA Safe-T ви можете надати своїм працівникам та підрядникам доступ до необх файлів, не знижуючи рівень безпеки.

safe-t
Masters of Access

sales@iitd.com.ua | +380-44-339-91-16 | **iitd.com.ua/safe-t/**