scConnect™ Security

scConnect is more secure than cloud services

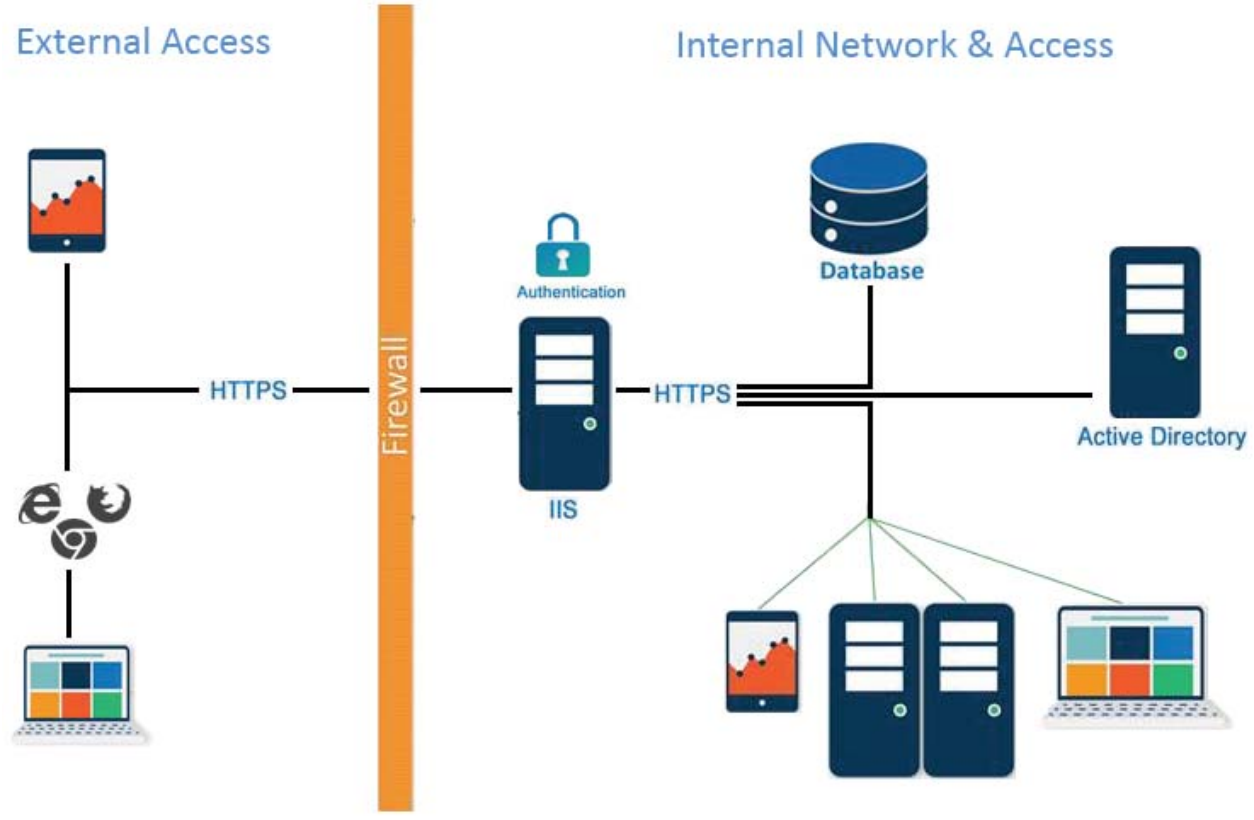
scConnect™ provides employees with a secure option for file sharing without losing control of your network. On-premises deployment provides the mobile access (BYOD) you want with the local administration and security you require—your own private cloud without the dangers of cloud-sharing providers. Centralized administration for IT governance, two-factor authentication, and complete audit trails ensure compliance with industry, government, and regulatory standards.

No Data is Ever Stored on Remote Servers

Cloud providers talk about encrypting "data at rest" because you have to move your data to their servers, where they have to keep it safe. You have no control over the security of your data once it leaves your network. With scConnect, no data is ever moved to "the cloud" or hosted on remote servers. Therefore, "data at rest" is secured by your private network security, inside your domain, under your control.

Is Data in Transit Always Secure over HTTPS?

When you access a website through HTTPS, the remote server is using a trusted certificate to encrypt the communication. However, that remote server and its certificate are out of your control. With scConnect, the control over your network is in your hands; it's your server and your trusted certificate, instead of someone else's server using the certificate they select.



4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

scConnect Provides a Single Point of Entry

When you invite others to access your data using consumer cloud providers, you are opening up every workstation in your organization to remote access by an external server. In contrast, the scConnect service is installed on workstations on which you want to allow sharing, and they speak only to your on-premises scConnect server. The scConnect server is the only connection to the outside world. That way, the network has only one point of entry and exit instead of one for every workstation in your organization.

An Additional Layer of Security

In addition to securing external access to the server, you must also ensure that the person you're giving access to your data is allowed to have access. In the enterprise, you already have multiple rules configured to decide who can have access and what data they are allowed to access. scConnect leverages your LDAP server, Active Directory, and (optionally) two-factor authentication to verify each of the users in your enterprise.

Using scConnect, you decide the internal access that you want to make available to a user. Based on internal permissions, the administrator dictates which users are allowed to share their files. Users prove they are allowed access with their Windows login and, if configured, two-factor authentication.

Mobile Security

scConnect mobile apps don't have any local storage. That is, scConnect never downloads a file all the way to permanent storage, as you would through the web browser. scConnect displays one file at a time for you to preview or to send to another app, such as email or printing. scConnect deletes the file as soon as you're done viewing it. On iOS devices, scConnect also encrypts an opened file.

Why is scConnect™ more Secure than Consumer Cloud Providers?

In summary, scConnect protects your data from unauthorized access with:

- On-premises, centralized administration for IT governance
- LDAP, Active Directory, and two-factor authentication (2FA)
- Complete audit trails ensure compliance with industry, government, and regulatory standards
- Single point of entry and exit to all data locations
- No data stored on mobile devices or remote servers

Contact Globalscape today to eliminate unsecure cloud providers from your network.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)