If you had to make one best decision for security, where would it be?

Secure File Transfer – The First Best Step

Put aside cyber security hype. The **most pervasive threat comes from humans and data-in-transit**. When employees and partners share information and data, they create a daily interchange for a thriving business. Today, this must be secure to ensure trust.

The first best step is to **protect the files**; so securely that it takes away the most vulnerable weak link of data-in-transit. If done easily and automatically, then the path to greater security is assured. Secure file transfer, when done right, lowers the risk of data breech tremendously.

Protecting the Peer to Peer Relationship

The value of a trusted relationship – whether in a private conversation, a critical moment of need, or protecting assets cannot be underestimated. We develop relationships and communicate in a unique way; secure data is very much like that too.

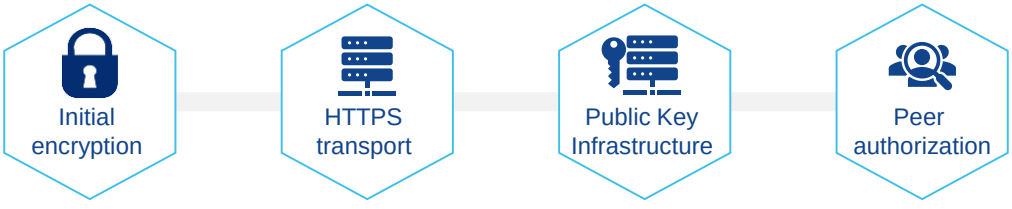
When we transfer data, it can be as safe as precious cargo. If we establish a **peer to peer relationship**, with a toolset that guarantees secure file transfer, we can substantially protect files and data.

Enter Safety4Data

Imagine a cyber approach where you can increase protection in five minutes… where you establish a trusted peer relationship and just pull files from your trusted place to theirs. Like an armored truck.

Safety4Data is a data encryption and transfer application which relies upon a secured, peer-to-peer virtual network that allows users to confidently exchange data with anyone in their network.

Layers of Security



Every file is secure from the moment of release to the moment of acceptance.

IT-CNS, Inc. 6401 Penn Avenue Pittsburgh, PA 15206 +1.404.542.6169 www.safety4data.com

A Bit More about Security

PKI works by assigning a pair of keys – public and private. Only the user who owns the keys has a private key, but the user's public key can be given to anyone. When using PKI, the user can secure not only the server authentication, but also the Safety4Data user authentication. In addition, users can encrypt/decrypt files using PKI.

During transfer, data is sent via Safety4Data's highly secure, encrypted HTTPS tunnel. The server is then authenticated by a server certificate, verifying the user is communicating with the legitimate Safety4Data application, not a spoofed server.

Files are encrypted and stored on Safety4Data servers until the recipient downloads them, at which time the files on the server is permanently deleted. Encryption certificates are acquired via "Certificate Authorities" and managed to optimize security.

Data security is created by using the Azure cloud server environment – technology which delivers a superior level of confidentiality, integrity, and stored data availability. This is completely managed by Safety4Data within the client peer-to-peer realm.

The Safety4 Data Elements

The Service

- Web administration local service is automatically installed in the background for PKI distribution and the files send/download process and the encryption/decryption process.
- Local service setup is done through the web administration and options can be done in the notification tray.
- PKI can be done with providers' certificates or optionally with the user's own certificates.

The Administration

- The local administrator creates virtual user network with either simple (all users can communicate only with local admin) or full (every user can communicate with all users).
- You can also create communication groups.

File size

- 200 MB or can be increased to 1GB or more.

User Flexibility

- Users work in their own OS with upload/download folders for drag-and-drop.
- Optional file sending with a context menu (right-click mouse operation)
- Optional direct files upload/download to/from web administration (for one-time communication with client) to provide more comfort to users.

Logging, Audit, Notification

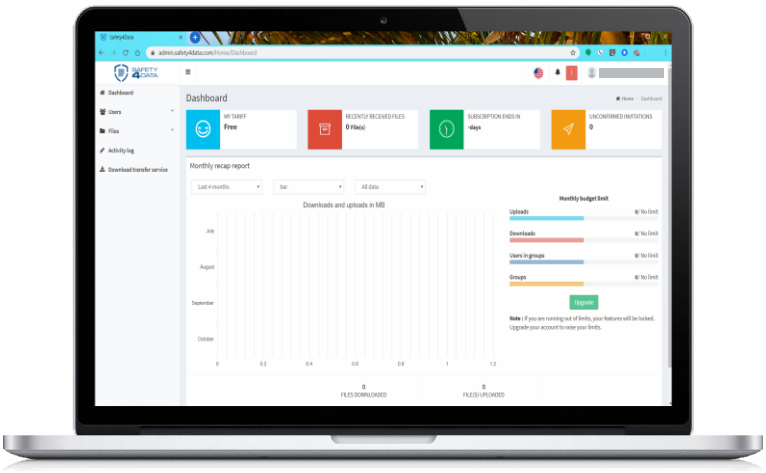
- Every file transfer is registered into the communication log to provide overview to users. An error log is provided if there are errors during the file encryption of transfer.
- A list of downloaded files (simple Download manager) with the name of file, information about sender and option to open a folder where the file is placed.
- Notification of email and system tray about upload/download files. Fully configurable.

Safety4Data Secure File Transfer

The Safety4Data Hosted Service

To use Safety4Data, you subscribe on a user basis and install a light footprint client. Everything else is taken care of for the secure transfer. Safety4Data is a set of software and tools on a hosted application, built on a client-server architecture to enable the creation of virtual secured networks.

Administration is an easy-to-use dashboard that manages files, users and subscriber settings for high file security.



Safety4Data Services

Safety4SERVICES represents the program, where file security experts can be engaged for projects and enterprise installations if needed. In addition, connection to existing data sources, API's and cloud-based systems can be done with the Safety4Data team. The hosted Safety4Data solution is fully supported with software and client upgrades as part of the program.

We offer personal Cyber Security Consulting services for small to mid-size businesses. We work directly with your business to fill the gaps and find affordable solutions to keeping your information secure and money saved. We understand that cyber security may not be a top priority, however, it is of the utmost importance to prepare, protect and be proactive, as opposed to assume you are safe, then be reactive to a breach that could be easily prevented.

Safety4CARE, is Safety4Data's software upgrade program that provides notification of software features and upgrades for the hosted solution.

Get Safety4Data

Start with the trial download HERE

Contact us at sales@it-cns.com