tresorit

Ebook

Secure file sharing and sync by design

Ebook

Secure file sharing and sync by design

Many organizations use file sharing and sync as a service to ensure convenient daily operations for employees. Companies are looking for features which allow users to: simplify and broaden the means of accessing files, cut down on IT efforts and resource costs, and centralize collaboration and file management. As organizations become more conscious of data confidentiality and user privacy concerns, convenience on its own is no longer enough. Although there are many file sharing and sync services available on the market, most of them only put a major emphasis on the convenience factor, while neglecting to implement the appropriate security measures necessary to ensure file security at all times.

01

Most cloud services tend to sacrifice security for the sake of convenience.

Most providers only apply in transit and at rest encryption as a means of file security. In reality, this means that files are only truly encrypted while stored long-term on a dedicated server. The problem with this is that file exchange infrastructures are highly complex and relying only on in transit and at rest encryption leaves files unprotected throughout the rest of the process.

Client files can leave the client unencrypted	**Transit** Unencrypted files travel via encrypted channels	**Sever** Files are unencrypted to be indexed & viewed	**Storage** First time files are actually encrypted

In transit

Files travel unencrypted while in transit as only the communication channels are encrypted and not the files within. This can be compared to tossing all files in secure transport vehicles. If the channel (aka the transport vehicle) is hacked, the data is easily readable by unauthorized individuals.

At rest

Although files are stored in encrypted format, providers tend to manage the file encryption keys within the same environment as the encrypted files. This creates a potential risk because if an attacker manages to gain access to the provider's storage system, finding the files and their corresponding keys is only a matter of time.

On the server-side

Files must remain unencrypted on the server-side for indexing, a process of marking file content which allows for file search and parallel collaboration. The downside is that in order to provide these convenient supporting features, organizations must allow providers to have complete access to their files. **External attackers and malicious insiders frequently attack the processing and indexing servers as they know that files are unencrypted while being managed.**

02

Tresorit secures the whole journey

Tresorit provides secure file sharing and sync by protecting files with end-to-end encryption. Tresorit stands out from mainstream file share and sync services by providing uncompromised security and great usability at the same time. Tresorit's end-to-end encryption and Zero knowledge features ensure that neither unauthorized individuals nor Tresorit as a service provider have the ability to access, view or manage your files.

Client Files can only leave the client in encrypted format	**Transit** Files are encrypted and travel through encrypted channels	**Sever** Files are encrypted on the server and labeled	**Storage** Stored files are encrypted and receive additional encryption

In transit

The risk of transferring files unencrypted is solved by Tresorit's automated client-side encryption procedure. Files are only allowed to leave any device once encrypted. Channel encryption in this case only acts as an added layer of security meaning that both the file and the channel it passes through are encrypted.

At rest

Just like in transit encryption, at rest encryption benefits from client-side encryption. This way, files are encrypted twice, and the encryption keys are only available on the client-side. This eliminates the risk of storing both files and keys in the same environment.

On the server-side

Tresorit servers are different compared to other providers' servers. With Tresorit all file processing functions are done on the client-side and files are transferred in data vaults. This is a security and privacy measure called Zero knowledge which ensures that Tresorit does not have access to the file's content. As a result, Tresorit servers act as data vault labeling and distributing tools which decide where data vaults come from and if they need to be stored or shared with recipients

03

In conclusion

Organizations often struggle to find the right balance between security and convenience when it comes to file sharing and sync. Many cloud services specialized in file management and exchange lean completely towards offering convenience supporting features above all else. This creates unnecessary risks for organizations as security is almost completely neglected.

Tresorit strikes a balance between convenience and security by providing an easy to use and end-to-end encrypted solution

04

About Tresorit

Tresorit is the end-to-end encrypted file sync and sharing solution which safeguards confidential information by design for businesses and individuals alike. Trusted by tens of thousands around the globe, our award-winning platform protects sensitive data and ensures compliance with end-to-end encryption. If you wish to learn more about Tresorit or how it guarantees end-to-end encryption and Zero-knowledge visit our website, request a demo or contact sales.