Secure external file-sharing for businesses

The ultimate guide to content collaboration in the cloud

tresorit

What's inside

The evolution of file-sharing for businesses

From file cabinets to cloud storage, file sharing and collaboration have come a long way. In the past, businesses usually relied on on-premise file servers to provide a central repository of information for their employees, while using email and chat services to share files externally. Despite the maintenance cost and administrative hassle, at the time, these file-servers were the ideal way for employees to share information and work on files together, because everything was designed and controlled in-house.

Then in the 2000s, cloud computing exploded in popularity and drastically disrupted the way people live and work in the digital age. Nowadays, more and more businesses are moving workloads to the cloud (or are even cloud-native). Employees have come to expect the same seamless working experience that consumers demand of their digital products – platforms which are easy-to-use and mobile, in a way that suits modern lifestyles and workplaces.

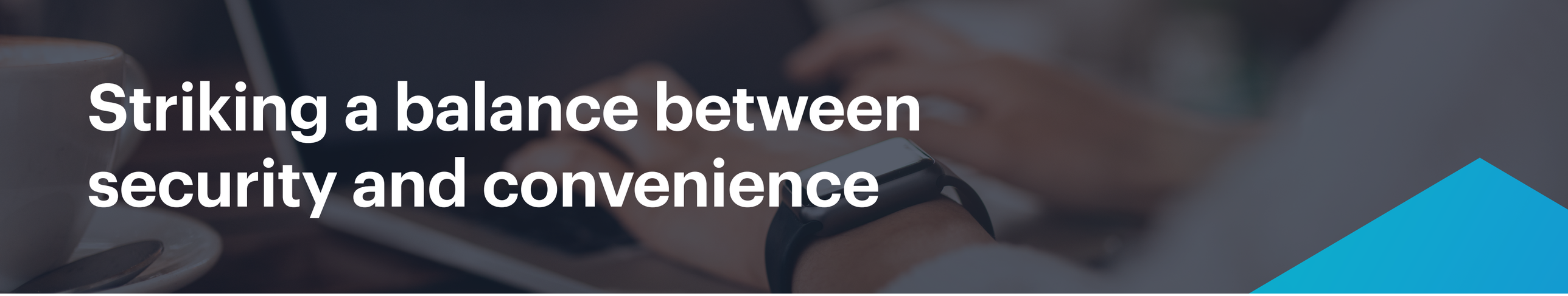
"83% of enterprise workloads will move to the cloud by the year 2020.

Forbes

At first, many organizations turned to mainstream cloud service providers and email providers to send files back and forth. They soon realized, however, that they couldn't use these services without compromising security for convenience. While suitable for exchanging personal, nonconfidential files, they fail to meet business-critical requirements for security levels, privacy standards and compliance regulations.

On top of that, another issue became clearer with every data breach that hit the headlines in the last years. In addition to being vulnerable to the usual data security threats (unauthorized access to files, information loss, data breaches) mainstream cloud service providers frequently view and scan their users' file content. They do this in order to offer certain features, generate targeted advertising and improve their services. Unfortunately, excessive vendor insights also create gaps in the data lifecycle, putting it at unnecessary risk.

Fast forward to now: the goal is to find an interface like the consumer cloud storage experience, while securing the whole data lifecycle. The main challenge for businesses looking to collaborate in the cloud is maintaining this secure, two-way communication channel between the business and external parties. The struggle generally stems from the options businesses are presented with when trying to choose between solutions for their needs. This paper explores these options, their advantages and disadvantages, and what the key to secure external file-sharing really is, as well as the right tools for secure content collaboration in the cloud.



Striking a balance between security and convenience

Businesses collaborate with external parties on a daily basis, ranging from client-facing, third party and business partner engagements. These engagements mainly consist of exchanging sensitive information across multiple departments and a significant number of individuals. Due to the broad scope in terms of the number of senders and recipients, and the fact that classified information is at stake, businesses often struggle when it comes to establishing a secure means of communication for exchanging sensitive files with external parties.

Option 1: Convenient but unsecure

Mainstream solutions such as emails, chat services and file sharing via public cloud repositories are all extremely convenient. They can be easily adopted by the business and don't require additional effort from external parties, although this ease-of use often comes at the expense of the overall security of the communication channel. In general, these solutions are meant for sharing nonconfidential information, and if used otherwise, there is a high risk of compromised security in the form of unauthorized access, disclosure and loss of sensitive files.

Option 2: Secure but inconvenient

Encrypted email, chat and cloud repository services do exist and are widely used on the market thanks to their exceptional security functions. That being said, they pose a challenge when it comes to convenient collaboration with external parties. The majority of these services demand that both the sender and the recipient own the same solution to maintain a secure communication channel. While this might be considered affordable by the business for internal use, it can get extremely expensive when used to protect all client facing communication and file exchange. From an external user's perspective, owning and paying for a service just to be able to securely interact with a single business may feel like an excessive investment of time and resources.

Option 3: The far from perfect compromise

This is a mix of the first two options and is the most common. In this case, a business would prefer to establish a secure way to share sensitive files, but also offer a convenient alternative for external collaborating parties. In theory it is excellent, but when it comes to execution, certain short comings become clear. Generally, businesses will share files via encrypted links, but will receive sensitive files through unsecure channels, making the communication secure in only one direction. The problem here is that the communication is only semi secure, and half the time sensitive files are still exposed to unnecessary security risks and threats.

> *The average cost of a data breach is $3.92 million as of 2019.*
>
> Security Intelligence

The key to secure two-way file-sharing

The right solution should empower businesses to establish a two-way communication channel while striking a balance between security and convenience. This is completely achievable using secure content collaboration solutions, which are cloud-based Software as a Service technologies.

What makes these solutions stand out from the crowd? The fact that they offer continuous file protection during the entire data lifecycle thanks to end-to-end encryption, while providing complete user privacy and full content ownership via zero knowledge protocol.

When using secure content collaboration solutions:

- External collaboration can occur in a secure environment where each file is individually encrypted and only accessible by authorized senders and recipients.
- Businesses are able to establish secure communication channels to collaborate with external parties in a convenient fashion.
- Secure communication is possible in both ways via encrypted file sharing and requesting options.

Meet Tresorit:
Tresorit is a Swiss, end-to-end encrypted, zero-knowledge content collaboration platform (CCP) designed to safeguard the digital valuables of individuals and organizations with the highest classification in the cloud. Tresorit's patented, award-winning technology protects files from unauthorized access, disclosure, and loss while enabling users to meet their global compliance requirements and stay in complete control of their data.

How can Tresorit help?
Tresorit empowers businesses to establish a secure, private, hassle-free and two-way means of communication between businesses and external parties to exchange sensitive files. This is made possible with end-to-end encrypted file sharing and requesting links.

Why Tresorit?
With Tresorit, businesses can securely exchange files with anyone, even external parties who don't own a subscription. With a safe, centrally managed communication channel, businesses can maintain the highest level of security in the cloud. To top it off, Tresorit offers frictionless integration with existing infrastructure, combined with powerful administrative capabilities for governing user and file activities.

> *"Clients were frustrated with encrypted email, and often sent sensitive documents in plain email. Sharing with Tresorit is easy. People appreciate that we handle their documents securely. It sets us apart from our competitors.*
>
> Guy Applebee
> Partner, Alpha Independent Mortgages

The key to secure two-way file-sharing

Here are a couple of the features Tresorit offers and the added security layers businesses should look for when collaborating in the cloud:

File sharing links: end-to-end encrypted links which allow businesses to provide sensitive files to external parties. Tresorit file sharing links offer added security layers including:

- Expiration date: Define the exact date and time that links are accessible for.
- Open limit: Define how many times shared links can be opened by recipients.
- Password protection: Request password input from recipients to mitigate unauthorized access.
- Email verification: Request email input from recipients to monitor and validate their identity.
- Revoke link: Instantly revoke access to links to mitigate human error and unauthorized disclosure.
- Access logs: Track link access based on time, date, utilized devices and user credentials.

File Request links: end-to-end encrypted links which allow external parties to securely share sensitive files with businesses they work with, without being required to own a product subscription. Tresorit File request links added security layers include:

- Set destination: Define where requested files should arrive once accepted.
- File review: Files first arrive in a review folder to be accepted or declined.
- Expiration date: Set links to expire after a specified amount of time.
- Email verification: Validate file providers via email verification.

Tresorit: An enterprise cloud standout with security features galore

TechRepublic

In conclusion

Tresorit's CCP empowers businesses to share and request sensitive files via end-to-end encrypted links when interacting with external parties. A simple, secure and private method to interact with clients, third party service providers and business partners on a regular basis.

tresorit

Meet our Sales Team

Eniko Mandzak
Head of Inside Sales

Paul Bartlett
Senior Customer Success Manager

Diana Fulop
Customer Success Manager

Balazs Judik
Customer Success Manager

www.tresorit.com

Regional Offices

Switzerland
+41 44 508 33 53

Germany
+49 89 2620 3681

Hungary
+36 70 679 32 83

United States
+1 (929) 999-7145

United Kingdom
+44 203 998 9521

About Tresorit

Tresorit is a Swiss, end-to-end encrypted, zero-knowledge content collaboration platform (CCP) designed to safeguard the digital valuables of individuals and organizations with the highest classification in the cloud. With headquarters in in Zurich, Switzerland, and regional offices in Germany, Hungary, the UK and US, Tresorit operates in the enterprise cloud storage and content collaboration platforms market.

Tresorit: The most secure way to collaborate. We encrypt everything, to know nothing.
Learn more at www.tresorit.com

Tresorit AG | Minervastrasse 3 | 8032 Zurich | Switzerland