tresorit

Highest level of cloud security for your business

Tresorit's End-to-End Encryption Technology Offers a New Level of Security for Cloud-Based File Collaboration and Sharing

End-to-end encryption

- Using end-to-end encryption, Tresorit encrypts every file and relevant metadata on your devices with unique, randomly generated encryption keys.
- These keys are never sent to our servers in unencrypted format. **The encryption is performed with a fresh, randomly generated 256-bit symmetric key** chosen by the client-side application. The encryption algorithm Tresorit applies is AES256 in CFB mode.

Cryptographic key sharing

- Tresorit's patented protocol ensures keys are shared automatically, without revealing them to anyone who has access to either the network
- Public key cryptography guarantees that even Tresorit cannot access the shared keys. This **key sharing is based on RSA-4096 with OAEP padding scheme used in group mode**, and PKI certificates, combining it with a tree of symmetric keys.

Zero-knowledge authentication

- Unlike other services, Tresorit never transmits or stores files, encryption keys and user passwords in unencrypted or unhashed form.
- **Tresorit only stores password in a salted hash format**, which we can authenticate users with. Tresorit never has access to your password in unencrypted form, even if our servers were hacked, your account would be safe from harm.

Client-side integrity protection

- Tresorit applies a Message Authentication Code (MAC) to each file, guaranteeing that the contents cannot be modified on Tresorit's servers.
- Tresorit applies a Message Authentication Code (MAC) to each file's content, with a key known only to the user's client and those they share the file with, but not by the server. **Tresorit uses HMAC-SHA512 with a random key** for each different file

PKI for all devices

- Tresorit uses **Public Key Infrastructure (PKI)** to authenticate each Tresorit user and their devices, without storing any information about their passwords.

Hardened TLS

- TLS (the successor of SSL) channel protection can be hardened through the use of client certificates. This method provides **public key-based security** when you connect to Tresorit servers.

Deutsches Rotes Kreuz

"Usability, secure encryption before the files leave the device, and end-to-end encrypted sharing. These are just 3 of the several reasons why we chose Tresorit. Tresorit is a big relief in sharing documents between our numerous facilities."
- **Gunnar Jasinski, Data Protection Coordinator, German Red Cross**

 | https://tresorit.com

tresorit Microsoft

Tresorit's End-to-End Encryption Technology Offers a New Level of Security for Cloud-Based File Collaboration and Sharing

Zero-knowledge end-to-end encryption

- Unlike other services, Tresorit never transmits or stores files, encryption keys and user passwords in unencrypted or unhashed form.
- Due to the strength of Tresorit's end-to-end encryption and security, breaking this protection would take several human lifetimes.

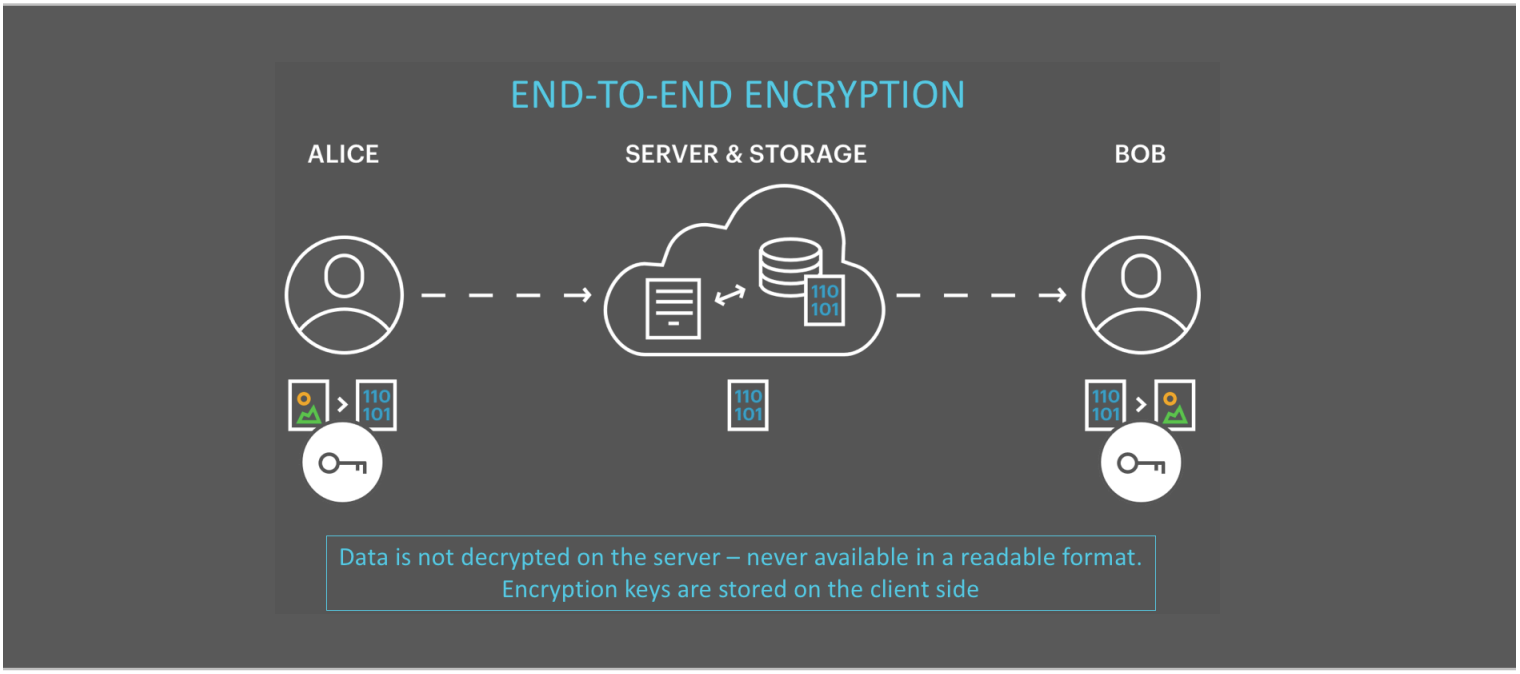
Highest level of security for your business

- Military-grade, AES-256 symmetric-key block encryption
- Patented sharable encryption: provides security of end-to-end encryption during the entire sharing workflow

Work securely and keep control of your confidential files in the cloud

Tresorit provides the security and file control businesses need to to collaborate securely in the cloud.

- End-to-end encrypted security
- Control and data governance for your organization
- Helps to demonstrate your compliance with GDPR
- Ease-of-use and deployment



Benefits

- Collaborate securely by storing, sharing and synchronizing confidential data with encryption
- Keep company data secure from external and internal data breaches
- Easily manage file control and permission levels within your organization
- Keep ownership of your data when working with external contractors

Why Tresorit?

Tresorit makes content collaboration secure for your business by combining end-to-end encrypted security, data governance features and ease-of-use. Using Tresorit's end-to-end encrypted cloud solution allows teams to collaborate securely by storing, sharing and syncing confidential files with ease.

 | https://tresorit.com

tresorit