Using Tresorit for file storage and editing

For organizations handling highly sensitive information where security outweighs convenience concerns, Tresorit provides privacy and security that mainstream providers cannot match. However, teams requiring extensive real-time collaboration may need to supplement with other tools or accept Tresorit's limitations, developing a policy dictating when to store data on Tresorit rather than on other systems, i.e. Google Drive.

What is Tresorit?

Tresorit is a secure cloud storage service based in Switzerland that uses end-to-end encryption and zero-knowledge authentication to ensure a very high level of security. As a Swiss company, Tresorit cannot be compelled to participate in mass surveillance by US or EU intelligence agencies.

How It Works

End-to-End Encryption: Your files are encrypted on your device and never decrypted until they reach your intended recipient - only you and anyone you authorize can decrypt the files. Tresorit uses AES-256, one of the most secure symmetric encryption standards available.

Zero-Knowledge: Tresorit doesn't store passwords or have access to unencrypted data. This means that even if Tresorit gets hacked or authorities demand your information, there's nothing to find on their servers.

Data Storage & Jurisdiction

- Primary Location: By default, data is encrypted and stored in data centers in Ireland and the Netherlands
- Legal Protection: Tresorit is subject to Switzerland's strong data protection laws

Key Differences from Google Drive

Feature	Google Drive	Tresorit
Encryption	Data on servers is not end-to-end encrypted, Google can decrypt	End-to-end encryption - files never decrypted on servers, only users can decrypt

Access by Provider	Google can access file content for various business purposes or to respond to a law enforcement request	Zero-knowledge - Tresorit cannot access your data
Government Requests	Must comply with U.S. government data requests, often with gag orders	Swiss jurisdiction protects against mass surveillance requests
Real-time Collaboration	Built-in document editing and collaboration	Primarily secure storage and sharing. But users can edit shared documents using Tresorit Drive on their local machines, with documents set to read-only while others are editing.

Tresorit Sharing & Collaboration Features for Teams

Secure Link Sharing

- Link Controls: Set expiry dates, download limits, and passwords on shared links
- Access Tracking: Enable access logs to track browsers, IP addresses, and email addresses that accessed your content
- Email Verification: Require recipients to verify their email before accessing shared content

Advanced Security Features

- Cooperative Links: Two-way collaboration allowing external partners to share, receive, and edit files through a single encrypted link without needing Tresorit accounts
- Watermarking: Add watermarks to shared videos and documents to prevent unauthorized re-sharing
- Download Control: Disable downloads on shared links while allowing preview

Team Collaboration

- Permission Levels: Three permission levels - Managers (read, change, re-share), Editors (read, modify), Viewers (read-only)
- File Access: Users can use Tresorit Drive to access files locally on their machines, or access cloud files directly from the Web.
- Folder Sharing: Direct collaboration in shared encrypted folders with granular access controls

Implementation Recommendations

Desktop Collaboration Strategy

1. Use Tresorit Drive for teams that prefer working in local documents rather than web interfaces

2. Implement Folder Structure with clear permission hierarchies for different materials
3. Leverage Cooperative Links for external collaboration without requiring accounts
4. Determine Storage Policies for sensitive documents that need to be stored and shared in Tresorit, rather than in Google Drive

Link Security Best Practices

- Always set expiration dates on shared links, especially for time-sensitive campaigns
- Use download limits (e.g., 5-10 opens) for highly sensitive documents
- Enable access logs for all external shares to monitor who accessed materials
- Implement password protection with separate communication channels for passwords

---