MEMSOURCE

Data Security

Enhancing Data Security with Memsource Cloud

Introduction

Most of our customers translate content that may be, and often is of a confidential nature. Therefore, data security is of the utmost importance to us. When potential customers explore Memsource, because it is a cloud-based solution, a key area of their scrutiny is usually security. This document provides answers to some of the most frequently asked questions relating to the security of Memsource Cloud.

Measures to Make Your Data Secure

We take a number of measures to protect customer data at Memsource, including physical security, data encryption, controlled access, our own corporate security, and others. Memsource is ISO certified to comply with the ISO Information Security standard (ISO/IEC 27001) and undergoes regular security audits by independent consultants. This document provides an overview of the measures we take to ensure the security of customer data.

MEMSOURCE

Physical Security

Access to Memsource facilities is controlled by a guard, 24/7 video surveillance and an access card system. However, our servers are never located in our office. We use high-security data centers to host Memsource Cloud servers, which have the following physical security measures in place: barbed-wire fencing, video surveillance and motion sensor systems. All systems are monitored by a 24/7 on-site surveillance team, and data center staff receive an RFID name badge to control their access.

Data Encryption

Customer data is encrypted, both in transit and at rest. Data in transit is data that, for instance, travels from Memsource Cloud servers to a user's web browser or a desktop application, such as Memsource Editor. Data at rest is data stored on our servers and is also encrypted. The reason for encrypting data in transit is to protect it when it travels across the web. Encrypting data at rest, even when it is stored in a high security data center, provides an extra layer of protection. Therefore, even in the case of an unauthorized user accessing our servers, the attacker would not be able to read the data.

Data Access

Customer data is protected by providing access only to authorized personnel. After signing up for an account in Memsource Cloud, an administrator user is created with the right to create additional users with appropriate access rights. Customers may also decide whether or not to grant access to Memsource technical support specialists to expedite the resolution of any technical questions or requests addressed to Memsource support staff.

Data Ownership and Privacy

In line with our Terms of Service, data that our customers upload to Memsource Cloud remains their sole property, and it is our utmost priority to keep their data private, confidential and secure. Content submitted to Memsource Cloud, including translations of that content, will remain the customer's sole property. Memsource will not share personally identifiable information with any third party without the customer's express consent, or unless compelled by applicable laws.

Redundancy and Backups

Redundant architecture ensures that data is not just secure but also accessible. Memsource Cloud's long-term availability is 99.8 percent. At the same time, we also maintain a high level of security for our redundancy and backup process. Again, all data is encrypted in transit and at rest. To ensure availability, all components are in a 2+ redundancy model and servers are located in two geographically distant data centers. Additionally, all data is secured through near real-time incremental backups as well as daily full backups to a geographically remote location.

MEMSOURCE

Adopting Memsource Cloud to Increase Security?

It is perfectly logical to have questions regarding security when exploring a new technology product. Will a cloud-based product increase or decrease the security of an organization's content during translation? The answer to this question will depend on two factors:

1. What is the security level of the organization's current translation process?
2. How secure will the translation process be when supported by Memsource Cloud?

Security of the Translation Process Before Adopting Memsource

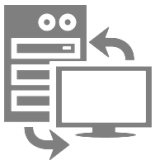
Most customers migrating to Memsource will have one of the below pre-Memsource translation setups. Let's explore their impact on security.

Scenario 1: No Translation Technology

Files for translation are distributed by email or FTP. Even if files are sometimes password-protected when emailed or when a secure FTP is used, security is still very low in this scenario. After the client hands over files to a translator or translation agency, the client loses all control over the files and their security. There is no control over who has access to the files, where the files are stored, etc. The translation industry is very decentralized, meaning that a file for translation can easily travel from the client, to a large translation agency, to a smaller, specialized translation agency, then on to its freelance translator, and so on. In this scenario, multiple copies of the file are stored on multiple devices with absolutely no client control of the data. In a situation such as this, the level of security is obviously completely unsatisfactory, however this is still a very common scenario in today's translation workflow.

Scenario 2: Desktop Translation Technology

Some clients own a desktop translation product where they maintain vital translation resources, such as translation memory, term base, the actual files for translation, etc. The typical scenario in this case would be similar to the previous, i.e. the desktop translation tool will export a bilingual file for translation which is then sent via email or handed over via FTP to the translation agency, and the same chain of file sharing follows. In this scenario, the translation agency will also need a translation tool that is able to process the bilingual file for translation. Most likely, the content of the file will be stored in the translation memory of the agency, along with its sub vendors, and the actual freelance translator that will do the translation. While a desktop translation product may increase translation efficiency, it causes additional security risks since the entire translation (both source and target) will be stored in several translation memories, most likely for a very long time. Also, the content will probably be re-used for the client's future translation, and also possibly for translations by other clients of the freelance translator. Very often, freelance translators keep just a single translation memory in which they store translations for all their clients.



Scenario 3: Client-Server Translation Technology

Client-server technology is a big step in the right direction. If a client owns a translation server product, the level of control should dramatically increase in comparison with scenarios 1 and 2. Unfortunately, the number of clients owning and maintaining a translation server product is very small, as significant financial resources are required, in addition to well-trained staff to operate and maintain the technology. Furthermore, most client-server products do not make it possible or easy to keep the same level of security throughout the entire translation workflow. Very typically, a bilingual file is exported for translation at some point, such as when a translation agency hands over a task to its freelancer. At this point, the level of security decreases dramatically and is similar to scenario 2 as the freelance translators processes the bilingual file on their PC locally, including the storing of all data into their translation memory.

Scenario 4: Memsource Cloud for Higher Security

Memsource has been uniquely designed to enhance translation security. With Memsource, data owners get full control over their translation material from start to finish. The data owner sets access rights, can revoke them at any time, and can prohibit downloads for highly confidential documents. Translators are directed to Memsource Web Editor for translation, which helps prevent any data from being stored locally on third-party devices. Data is stored only on Memsource Cloud servers, which are located in highly secured data centers. Our customers' data is encrypted, both at rest (when stored on our server) and in transit (i.e. when being sent to a user's browser). This includes highly decentralized scenarios in which translation tasks are outsourced to a translation agency that further outsources it to its sub vendors. In this way, Memsource Cloud provides some of the most effective security currently to be found in the translation industry.