

# Security and Technical Overview

## We believe in being good citizens in the Salesforce ecosystem.

Customer security and privacy are at the forefront of every decision we make regarding development, support and expansion of Cloudingo. Managing the security of the Cloudingo application as well as all systems and data that make up Cloudingo are our top priority. We uphold the highest security standards, and have passed Salesforce's rigorous audit every year without fail.

- ✓ Communicates with Salesforce via API calls
- ✓ Your data is never stored nor cached
- ✓ Sophisticated and strict password policy
- ✓ Random penetration testing and annual audits
- ✓ Securely rests behind server firewalls

## HOW IT WORKS

When records are modified in Salesforce, the Cloudingo agent (which is 100% Force.com and sits inside Salesforce) looks at what filters the user has setup inside the Cloudingo Web Portal. If the records are in the scope of the filters, the agent logic fires.

When you click on a group of duplicate records, Cloudingo makes a real-time API call to Salesforce to show you the records side-by side. Once a merge takes place, the Cloudingo Web Portal calls the native merge command.

The actual data is not cached, so as soon as you move off that screen, your data only exists in Salesforce.

## ACCESS TO DATA

We receive some stats from Cloudingo, but they are only raw numbers based on the filters within our application. (This is equivalent to Salesforce knowing how much data is stored in the org.)

From our logs, we can report on the configuration of Cloudingo filters as well as their results in terms of raw numbers (numbers of duplicates identified), but no other details.

Furthermore the Cloudingo team members cannot see your data. The only exception is if you grant our support engineers "Support Access" to the Cloudingo Agent so that they can login and troubleshoot issues.



registered ISV  
partner

## We're a registered Salesforce ISV (Independent Software Vendor) partner.

This means we must meet Salesforce's strict partnership requirements, including periodic security reviews. We proudly exceed the vigorous security standards every year. For you, this means that you can trust that you're working with a loyal, trustworthy company. (Read more about Salesforce's [security requirements here.](#))

## DATA STORAGE

Cloudingo stores very little data, only field maps and the data from the primary field used to establish matches.

When opening a group of duplicates, Cloudingo makes a real-time API call to Salesforce to display the field data to the user. Once the group is closed, the data is released.

Salesforce credentials are stored in Cloudingo. They are fully encrypted. Once saved, they can be updated but never viewed again.

## RESOURCES & DATA USAGE

When the merge grid is viewed in the Cloudingo Web Portal, Cloudingo employs a sophisticated algorithm to make a secure Salesforce API call (via either OAuth or with the stored AES 256 encrypted credentials for the user) to pull the data in real-time for user review. Cloudingo uses the minimum amount of resources possible while balancing the actual speed of the responses back from Salesforce.

Cloudingo strives to get the most out of every API call so that any other applications or custom codes in Salesforce you may use also have plenty to work with. This is why we work hard to performance tune the native agent and save resources whenever possible including CPU cycles, heap size, message size, DML rows, "bulkified" triggers, etc.

Cloudingo automatically switches between "real-time" index mode and "batch" index mode based on user preferences and available resources. You can also easily apply hard limits on resources.

## HIGHEST STANDARDS

Any and all information that you see and interact with inside Cloudingo is protected using industry standard 256-bit SSL encryption.

Every year we have passed Salesforce's intensive audit without fail. Internally we perform security audits each time a release goes out (often times more frequently).

## SERVERS & COMPLIANCE

The web portal runs on a SAS-70 type II compliant infrastructure at one of the nation's largest hosting providers. Cloudingo is hosted inside of this data center on dedicated servers with dedicated firewalls. All the standard physical security features are present: biometric access controls, intrusion detection, redundant power feeds and generators, fire suppression, climate control, etc.

The Cloudingo servers are whitelisted, and the Salesforce servers are the only servers allowed to communicate with the Cloudingo web service end-points. In addition, our company, our team and all of our hardware are located in the USA. We do not outsource anything.



symphonic source

## ABOUT SYMPHONIC SOURCE

Symphonic Source Inc.'s mission is to provide customers with resources to manage the exponential growth in data, saving time and money, and adding efficiency. Symphonic Source, Inc. delivers a full range of data management and data quality tools and services, from data cleansing and integration, to deduplication and standardization, enabling users to realize the full potential of cloud-based and service-oriented architectures (SOA).

Symphonic Source's self-serve data quality products, Cloudingo, DupeCatcher, and Cloudingo Studio make it possible to eliminate and prevent duplicate records and manage data in the Salesforce CRM database. Its customized data management services make it possible for small to enterprise level organizations to fully take advantage of their investment in valuable data resources.