CopyStorm Security Considerations and Behavior

Gregory Smith, Capstorm CTO
Revised: January 2018

Table of Contents

Overview....1
Network Communication....1
  Salesforce Communication....2
  Customer Database Communication....3
  Capstorm License Server Communication....3
Data at Rest....3
  Salesforce BASE64 Encoded Columns....4
  License Files....4
  User Preference Files....4
  CopyStorm Job Configuration Files....4

Overview

As a customer hosted application running totally with a customer's firewall, CopyStorm security issues are primarily related to communication with three separate entities:

- Salesforce
- A Customer Supplied Database
- The Capstorm license server: https://license.capstorm.com

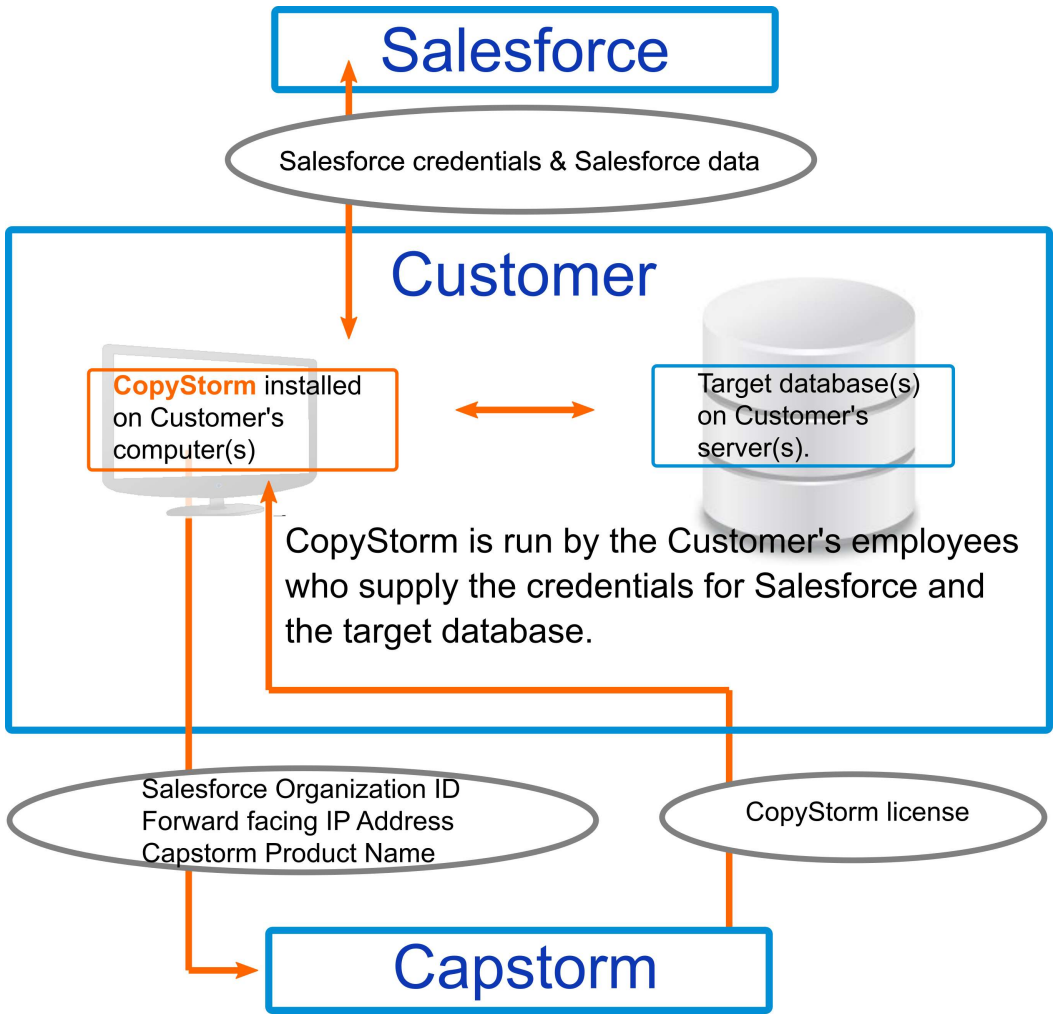
CopyStorm also maintains configuration information stored on a local file system outside of the customer supplied database.

The following document describes the security measures in place for each type of communication and the options available to a customer in order to control the applied level of security.

Network Communication

The following diagram illustrates the network communication that occurs when using CopyStorm. There are two key points to notice:

- All communication of Salesforce data happens between a customer controlled computer and Salesforce's data centers.
- The only communication to a Capstorm owned computer is to obtain a software license.



The next few subsections describe the security aspects of each network component in detail.

Salesforce Communication

CopyStorm communicates to Salesforce using their standard APIs – SOAP, REST, and BULK.

- All communication occurs over https as prescribed and dictated by Salesforce.
- The level of capabilities CopyStorm has within Salesforce is determined by the Salesforce credentials provided by a customer. The only access that is required for the Salesforce credentials is the ability to read data – no insert/update/delete permissions are required.

  The precise minimum permission requirements are described in the following article: https://learn.capstorm.com/copystorm-menu/storm-frequently-asked-questions/item/185-cstorm-faq-minimum-permissions

Note: Salesforce enforces all data visibility, encryption rules, etc, regardless of the communication method. A user with a web browser has the same level of data access as the same user communicating with Salesforce via an API.

Customer Database Communication

CopyStorm stores all data read from Salesforce within a relational database supplied and managed by a customer. At no point does any Capstorm owned server contain customer Salesforce data; all data is delivered directly from Salesforce and then stored in a customer's database.

CopyStorm performs all database communication via a database vendor supplied JDBC driver and the style of communication between CopyStorm and a database is determined by the connection string supplied by a customer when setting up the database connection. Most companies communicate with their database without using encryption but most databases supported by CopyStorm also support database communication across an encrypted tunnel. Most importantly, the customer controls how database communication is managed.

CopyStorm requires database credentials that own a schema in a relational database. Other than ownership of a schema, no special permissions are needed. Schema ownership is necessary because CopyStorm will create/alter table objects within its schema as part of the process of keeping the relational database in sync with the corresponding table structure in Salesforce.

Capstorm License Server Communication

When CopyStorm fails to find a local license or the local license has expired, it will call out to https://license.capstorm.com and request a new/updated license. The information sent to Capstorm's license server is minimal and is insufficient to identify a customer (by anyone but Salesforce).

The data sent to https://license.capstorm.com and the associated response is described in the following article:

- https://learn.capstorm.com/copystorm-menu/storm-frequently-asked-questions/item/53-copystorm-license-management

If a customer decides to block communication to the Capstorm license server, Capstorm will handcraft a license and send it to a customer via email. This approach has a few downsides:

- When CopyStorm software is upgraded to a new point release, Capstorm support will need to be contacted for a new license.
- Each use of CopyStorm on a new Sandbox requires a contact with Capstorm support.

Nearly all Capstorm customers opt to allow communication with https://license.capstorm.com.

Data at Rest

There are four classes of data kept by CopyStorm at rest on a local file system.

- Salesforce BASE64 encoded columns
- License files
- User Preference files
- CopyStorm Job Configuration files.

Salesforce BASE64 Encoded Columns

When any table containing a BASE64 column is downloaded from Salesforce, the BASE64 columns are persisted in a system temp directory before they are migrated to a database. Once migrated, the persisted data is deleted from the file system. The location of the temporary directory can be controlled by the customer.

In Salesforce, columns designed to contain a lot of data (more than 32K) or binary data are stored as BASE64 encoded strings. This primarily impacts Salesforce Attachment and ContentVersion objects. To minimize the size of SOAP and REST communication envelopes, BASE64 columns are streamed from Salesforce directly into a temporary file and then streamed to a database (when the database supports the feature – not all do).

The file system temporary storage of BASE64 columns can be disabled with a small XML file configuration change at the cost of potential memory requirements for the CopyStorm application.

License Files

CopyStorm persists license information generated by the Capstorm license server into a simple text file named *license.txt*. The information would be useless if exposed to someone outside of a customer's organization and contains no information useful to access customer's systems.

The data stored in a Capstorm license file is described in the following article:

- https://learn.capstorm.com/copystorm-menu/storm-frequently-asked-questions/item/53-copystorm-license-management

User Preference Files

CopyStorm persists user preferences like application window size and recently opened configuration files to the directory $HOME/.capstorm. All user preference files are plain text and do not contain security related information.

CopyStorm Job Configuration Files

Information which controls the behavior of a CopyStorm backup is stored in job configuration files (extension .copyStorm). Though the bulk of a job configuration file consists of Salesforce table names and backup process configuration, a job configuration file may optionally contain:

- Salesforce and/or Database passwords encrypted with DES-256

The choice of whether to store encrypted passwords is up to a customer as is the decision of whether the entire configuration file should be encrypted at rest.

CopyStorm also supports the specification of any password as part of application launch and how the password is obtained can be determined by the customer.