Metazoa Security Policy

Customer Information about Privacy and Security

The Snapshot Change and Release Automation product was explicitly designed to protect customer privacy and security. This whitepaper discusses the unique advantages of the product's architecture and also explains the security and privacy polices put in place by Metazoa as a company.

Source Code Control

There are two parts to the Snapshot Change and Release Automation product. First, the Metazoa Player is a compiled desktop application written in C that implements a security sandbox designed to protect the client computer, the local file system, and private network assets. Second, the Snapshot Document is a binary file which contains all of the scripted content, user interfaces, and other graphics associated with the actual application. The Metazoa Player is similar to a Java or .NET virtual machine, and the Snapshot Document is similar to a Java jar file or .NET assembly.

The Metazoa Player was written by an engineering team led by Bill Appleton, and different version of this code base have been in use for 20 years. The multi-platform code base is used to build two separate executable programs, one for Microsoft Windows and the other for Apple Macintosh. Both versions of the Metazoa Player are code signed to prevent tampering with the executable.

The Metazoa Player was carefully written to minimize and abstract contact with the local machine, but also to allow access to certain external web based assets and local desktop files in a sandbox folder. This environment provides an extra layer of security for the customer, their desktop computer, and the local network. The Metazoa Player was designed to be a secure container for potentially untrusted applications.

The Snapshot Document contains the scripted content, user interfaces, and other graphics associated with the actual application. When new and improved versions of Snapshot become available, a new Snapshot Document is downloaded to the Metazoa Player for execution. This provides a simple and secure method of managing application updates. The download process is visible to the customer. The documents are scanned for irregularities, and a checksum is used to prevent tampering.

The Metazoa Player is mature and rarely updated. The SnapShot Document is updated at least three times a year to coincide with Salesforce API releases. There may be additional SnapShot Document updates throughout the year to address product enhancements, bug fixes, and performance improvements.

Metazoa maintains a read-only file server at http://www.metazoa.net where the Metazoa Player can be downloaded. When the desktop application is started, the latest Snapshot Document is downloaded from the same location. Physical access to the Metazoa Player and the latest Snapshot Document are controlled through SFTP with a client key on a secure computer. Here are the download locations for the Metazoa Player installation program:

Microsoft Windows

https://www.metazoa.net/codebase/MZInstall32.exe
https://www.metazoa.net/codebase/MZInstall64.exe

Apple Macintosh

https://www.metazoa.net/codebase/MZInstall32.pkg
https://www.metazoa.net/codebase/MZInstall64.pkg

Serverless Architecture

When a customer logs into their Salesforce account, Metazoa uses the Data, Metadata, or Tooling API to manage the associated org. This creates a session ID that the product uses to communicate directly with salesforce.com. All communication is conducted between the customer's personal computer and their salesforce.com account.

The customer's private data, username, password, and session ID are not transferred anywhere except back and forth from their personal computer to their Salesforce account. The session ID is used for communicating directly with Salesforce while the application is running and is discarded when the application terminates. The customer's private salesforce data is not transmitted, duplicated, or cached on any other server or database whatsoever.

The Metazoa Player uses HTTP POST over SSL for network communication. This is the same network protocol that the Salesforce web application uses to run in a browser, except Metazoa is communicating to Salesforce with XML SOAP instead of HTML documents. The diagram below illustrates this architecture.

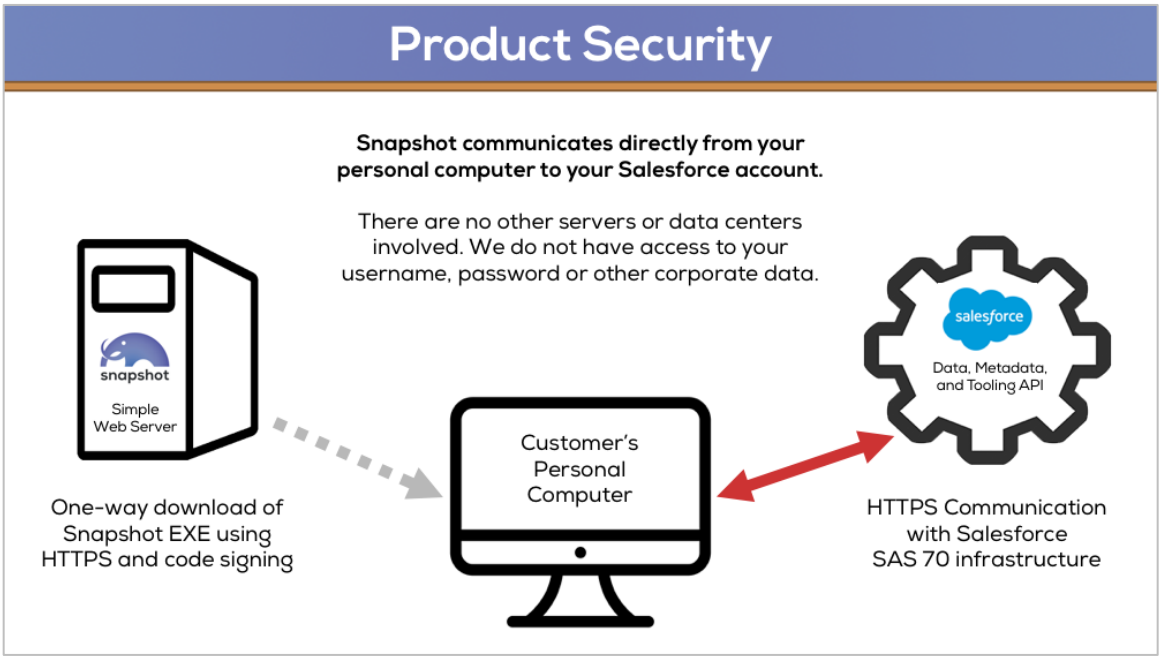

Figure 1: Snapshot Security Architecture

Metazoa Security Policy

The Snapshot Change and Release Automation product communicates directly between the customer's personal computer and their salesforce.com account. All transactions take place with salesforce.com API services and are conducted using the SSL protocol. All transactions conform to the AppExchange API security policy, and the policy that administrators have established for users in their Salesforce account. The read-only Metazoa file server is only used for the initial download of the Metazoa Player desktop application and after that a Snapshot Document that delivers product updates.

Metazoa Privacy Policy

The Snapshot Change and Release Automation product communicates directly between the customer's personal computer and their salesforce.com account. None of the customer's personal data is sent to Metazoa, Inc. or stored on any other server. Any personal data that the customer explicitly send to Metazoa, for example to request product information, will be used solely for product licensing, customer relationships, and technical support. The customer's personal information will never be transferred to a third party or become linked to any database external to Metazoa.

Contact Information

Author
Name: Bill Appleton
Email: bill@metazoa.com

Phone Numbers
Toll Free: 1-833-638-2962

Website:
https://www.metazoa.com/