Snapshot Security Policy

Customer Information about Privacy and Security

Metazoa is a publisher of software products and utilities for Salesforce administrators. Our flagship product is Metazoa Snapshot. Snapshot helps Salesforce Administrators remove technical debt, optimize security, improve compliance, become more productive, and lower the total cost of org ownership. Snapshot also provides tooling for org splits, clones, and merges. Snapshot has passed the Salesforce Security Review process. Here is a link to the AppExchange listing for Snapshot:

https://appexchange.salesforce.com/appxListingDetail?listingId=a0N300000016YhyEAE

Our Snapshot product has been explicitly designed to protect customer privacy and security. This whitepaper discusses the unique advantages that are inherent in the Metazoa software architecture. This whitepaper also explains the security and privacy polices put in place by Metazoa as a company.

Metazoa Player

There are two parts to any Metazoa software product. First, the Metazoa Player is a 64-bit desktop application written in compiled C that implements a security sandbox designed to protect the client computer, the local file system, and private network assets. Second, the Metazoa Document is a binary file which contains all 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 Metazoa 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.

Metazoa Document

The Metazoa Document contains the scripted content, user interfaces, and other graphics associated with the actual product. When new and improved versions of a product become available, a new Metazoa 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 code signing is used to prevent tampering.

The Metazoa Player is mature and rarely updated. The Metazoa Document is updated at least three times a year to coincide with Salesforce API releases. There may be additional Metazoa Document updates throughout the year to address product enhancements, bug fixes, and performance improvements. Customers can opt out of automatic upgrades if desired.

Product Distribution

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 Metazoa Document is downloaded from the same location. Physical access to the Metazoa Player and the latest Metazoa Document is controlled through SFTP with a client key on a secure computer. Bill Appleton is the gatekeeper for changes on this server. The customer can also choose to have the product delivered by mail on CD-ROM if desired. Here is the installation page for Metazoa Snapshot:

Install Snapshot

https://www.metazoa.net/install/snapshot.html

Microsoft Windows Player

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

Apple Macintosh Player

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

Serverless Architecture

When a customer logs into their Salesforce org, the Metazoa client application retrieves a Session ID that is used to communicate with the Data, Metadata, and Tooling API. All communication is conducted directly between the customer's personal computer and their Salesforce org. Customer credentials are stored in ephemeral RAM memory and discarded when the application terminates. Data and metadata used by the product are stored in a secure folder on the customer's local hard disk. The customer's private Salesforce data and metadata are not transmitted, duplicated, or cached on any other server or cloud that is outside of the customer's environment.

The code signed Metazoa Player is downloaded once from the file server at www.metazoa.net. The Player can also be delivered by mail on CD-ROM if desired. The Metazoa Player uses TLS 1.2 and HTTPS for network communication with the Data, Metadata, and Tooling APIs. This is the same network protocol that the Salesforce HTML web application uses to run in a browser, except Metazoa is communicating with XML instead of HTML documents. The diagram below illustrates this architecture.

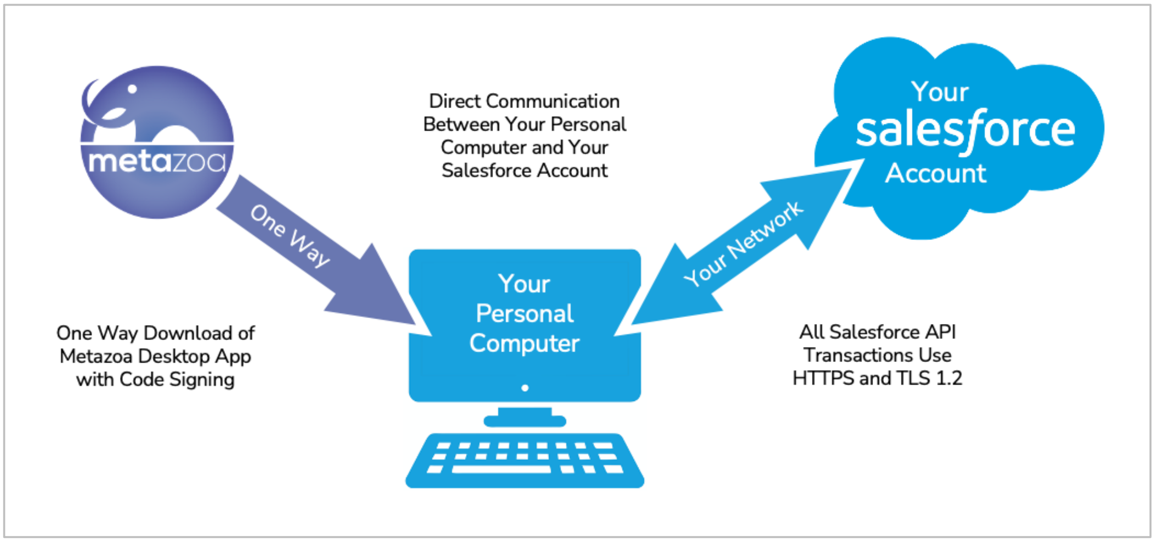
metazoa
One Way
One Way Download of Metazoa Desktop App with Code Signing
Direct Communication Between Your Personal Computer and Your Salesforce Account
Your Personal Computer
Your Network
Your salesforce Account
All Salesforce API Transactions Use HTTPS and TLS 1.2

Figure 1: Metazoa Player Security Architecture

The Metazoa Player runs on the customer's personal computer or virtual machine infrastructure and communicates directly with their Salesforce account. There is no intermediate cloud or database. Metazoa has the same modern desktop architecture as Slack, Tableau, Salesforce DX and Visual Studio Code. Metazoa software products are both more interactive and more secure than alternative architectures that can potentially expose your administrative credentials and private data to the open Internet.

Virtual Machine Installation

The Metazoa Player can be run on a Virtual Machine in the cloud or behind a corporate firewall instead of a personal computer. This option allows greater control over the computing environment. All customer data and metadata are stored on the Virtual Machine's hard disk. All Internet connectivity takes place on the Virtual Machine's network. During professional service engagements, a Virtual Machine can be used to keep all customer data and metadata inside the customer's computing environment.

Customer Computer

Administrative tools such as Data Loader, Salesforce DX and Visual Studio Code store org data and metadata on the customer computer. Administrative users with the Modify All Data permission can download this information in many ways. Customers should be sure these computers have a secure password. Technologies such as FileVault and BitLocker can be used to encrypt information at rest. Metazoa products have full support for OAuth, named credentials, and multi-factor authentication. These technologies should be used to reduce the reliance on client passwords.

Storage Options

The Metazoa Snapshot product has data migration capabilities that are used for moving data between orgs and seeding sandboxes. This feature is similar to Salesforce Data Loader and uses the Bulk Data API. When this feature is used data records are stored on the customer computer. Customers that do not want data records being handled in this manner can turn off Snapshot's data migration feature. All the different Snapshot data and metadata management capabilities can be individually turned on and off to prevent accidents or tailor the usage of the tool based on customer preferences. All data and metadata files are stored in the Metazoa Folder. This information is easy to archive, backup, and delete as needed.

Regulatory Compliance

The Metazoa Player has been architected to ensure data privacy. All customer data and metadata remain in the customer's computing environment. The fact that there is no intermediate cloud or data center helps ensure that privacy regulations such as HIPAA and GDPR are inherently followed. The Metazoa Snapshot product follows the ALCOA principles for GxP. The reports that Snapshot generates are:

- Attributable to an individual using Salesforce authentication
- Legible documents including HTML, PDF, EXCEL, and PNG
- Contemporaneous based on the Salesforce server timestamp
- Original and dynamically generated by the Snapshot product
- Accurate results tested in thousands of different Salesforce orgs
- Permanent documents saved to hard disk or Salesforce Content

Snapshot also conducts metadata deployments and data migrations. These org transformation operations also support GxP principles:

- Traceability: Snapshot maintains and stores deployment history logs
- Accountability: Changes are tagged using Salesforce authentication

External Integrations

Metazoa products integrate with some external applications and API services. The external applications must be installed on the desktop computer for successful integration using the Command Line interface. These external applications include:

- Git - for integration with Git Repositories
- PMD - for the static analysis of Apex Classes
- Salesforce CLI - SFDX support of Developer Projects

If for any reason a customer is concerned about the security characteristics of these external applications, then they should be uninstalled from the desktop computer or laptop.

Metazoa products also integrate with some API services. If for any reason a customer is concerned about the security characteristics of these API services, then access can be turned off with the Workspace Manager. This permission prevents Metazoa from calling the given API service.

- Google Search API - for searching Error Messages and org management support
- Stack Exchange API - for searching Error Messages and org management support
- OpenAI Developer API - for Artificial Intelligence and org management support

In the case of OpenAI grounding data is used in some circumstances. Grounding data includes packets of Data and Metadata required for intelligent analysis. The OpenAI API does not store prompts or grounding data for any purpose. In particular, the developer API does not use prompts for training. The Snapshot preferences interface allows the customer to enter their private developer key for OpenAI if desired. The service can also be enabled or disabled in the preferences interface. Find more information below.

https://pmd.github.io/
https://cli.github.com/
https://developer.salesforce.com/tools/sfdxcli

https://api.stackexchange.com/
https://platform.openai.com/docs/introduction
https://developers.google.com/custom-search/v1/overview

Compliance Controls Matrix

Control Category	Snapshot Approach
Encryption in Transit	All communications with Salesforce APIs use **TLS 1.2** and **HTTPS** protocols to ensure encryption during transmission.
Encryption at Rest	Customer-controlled. Data and metadata are stored **locally** on customer machines or virtual environments. Customers are encouraged to use operating system encryption tools such as **BitLocker (Windows)** or **FileVault (MacOS)**.
Access Control	**Inherited from Salesforce**: OAuth, Single Sign-On (SSO), Named Credentials, and Multi-Factor Authentication (MFA) are fully supported. Metazoa does not store or manage user credentials.
Authentication	Snapshot relies entirely on **Salesforce authentication** systems. No independent authentication mechanism is introduced by Metazoa.
Data Storage	All customer data and metadata are stored **locally**. Metazoa does not store, cache, or transmit customer information to any external server or cloud.
Backup and Recovery	**Customer-controlled**. Customers are responsible for backing up local data if desired. Metazoa provides clear guidance on folder locations for easy backup or deletion.
Incident Response	Customer environments are isolated. Any issues are reported directly through Metazoa technical support (**9 AM – 5 PM Pacific Time**). To date, there have been **no security incidents** involving Snapshot.
Software Integrity	All Metazoa software executables are **code signed** to prevent tampering. Updates are delivered over secure HTTPS and verified prior to execution.
Vulnerability Management	Internal **QA, security testing, and automated testing** are conducted before every release. The build process is tightly controlled by Metazoa engineering leadership.
Disaster Recovery	If Metazoa's update server becomes unavailable, Snapshot continues functioning locally. Only the ability to receive product updates is delayed. No disruption to daily operations.
External Services	External API integrations (Google Search, Stack Exchange, OpenAI) are **optional and customer-controlled**. Customers can disable them at any time through application preferences.
Compliance Alignment	Snapshot's serverless local architecture naturally supports regulatory compliance with **HIPAA**, **GDPR**, and **GxP ALCOA** principles by ensuring data remains entirely within the customer's environment.

Metazoa Security Policy

All Metazoa software products communicate directly between the customer's personal computer and their Salesforce org. Metazoa does not have access to any customer data, metadata, or credentials. All transactions take place with Salesforce API services and are conducted using TLS 1.2 and HTTPS. All transactions conform to the Salesforce API security policy. All transactions are further limited by the policies that customers have established for their Salesforce org. All the Metazoa software products available on the AppExchange have passed the Salesforce Security Review.

Metazoa Privacy Policy

All Metazoa software products communicate directly between the customer's personal computer and their Salesforce org. Metazoa does not have access to any customer data, metadata, or credentials. Our Snapshot Org Management product uses the Salesforce License Manager to administer customer access. The other products are licensed to an individual org and the associated sandboxes. Customer information is used solely for product licensing, feature roadmap, and technical support. Personal customer information will never be transferred to a third party or become linked to any database external to Metazoa.

Contact Information

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

Company:
Metazoa
1 University Avenue
Los Gatos, CA 95030

Phone:
Toll Free: 1-833-638-2962
Local: 1-408-660-3399

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