DreamFactory Software, Inc.
1999 South Bascom Avenue, Suite 928
Campbell, CA 95008

DreamFactory Security Whitepaper

Customer Information about Privacy and Security

DreamFactory Software publishes rich applications for salesforce.com. All of our products for salesforce use the DreamFactory Player, including SnapShot, Monarch, DreamTeam, and DreamFactory Utilities. The DreamFactory Player is designed to protect your privacy and security. This whitepaper discusses the unique advantages of our architecture and explains the security and privacy polices put in place by DreamFactory Software as a company.

Server-less Architecture

DreamFactory Software maintains a website at http://www.dreamfactory.net where the DreamFactory Player can be downloaded. This is a highly secure Linux server managed by Rackspace that is only used to download our products. There are no other "moving parts" on this website. The home page of this server simply redirects to our corporate site at http://www.dreamfactory.com. The server has a VeriSign SSL Certificate to provide for secure downloads.

The DreamFactory Player is a desktop application that runs on Microsoft Windows and Apple Macintosh. The application itself is code-signed for both Windows and Macintosh to identify the publisher and prevent tampering. All of our different salesforce.com products take advantage of this runtime player. The DreamFactory Player requires a one-time download in order to access the salesforce.com products. Here are the Player download locations:

Microsoft Windows

https://www.dreamfactory.net/codebase/DFInstall32.exe
https://www.dreamfactory.net/codebase/DFInstall64.exe

Apple Macintosh

https://www.dreamfactory.net/codebase/DFInstall32.pkg
https://www.dreamfactory.net/codebase/DFInstall64.pkg

The individual salesforce.com products all run inside the DreamFactory Player. The DreamFactory Player implements a security sandbox that protects local files, other documents, and private network assets. The architecture is similar to a Java or .Net virtual machine.

The player is carefully written to minimize and abstract contact with the local machine, but to also allow access to certain external web based assets or local desktop files under user control. This environment provides an extra layer of security for each salesforce.com product.

New and improved versions of our salesforce.com products become available from time to time and they are brought down to replace the existing version inside the DreamFactory Player. This provides a simple and secure method of managing application updates. The download process is visible to the customer.

The salesforce products log into an individual user account using the salesforce.com Data or Metadata API. This creates a session ID that we use to communicate directly with salesforce.com. The communication method is HTTP POST over SSL. We conform to the security requirements for the salesforce.com Data and Metadata API where XML documents are exchanged with a remote endpoint. All communication is conducted directly between your personal computer and your salesforce.com account.

Your private data, username, password, and session ID are not transferred anywhere except back and forth to salesforce.com. Your session ID is used for communicating directly with Salesforce while the application is running and discarded thereafter. Your private salesforce data is not transmitted, duplicated, or cached in any other server or database. All communication is conducted directly through an encrypted Secure Sockets Layer pipeline with the salesforce.com SAS 70 certified servers that host your account. The diagram below illustrates this process.

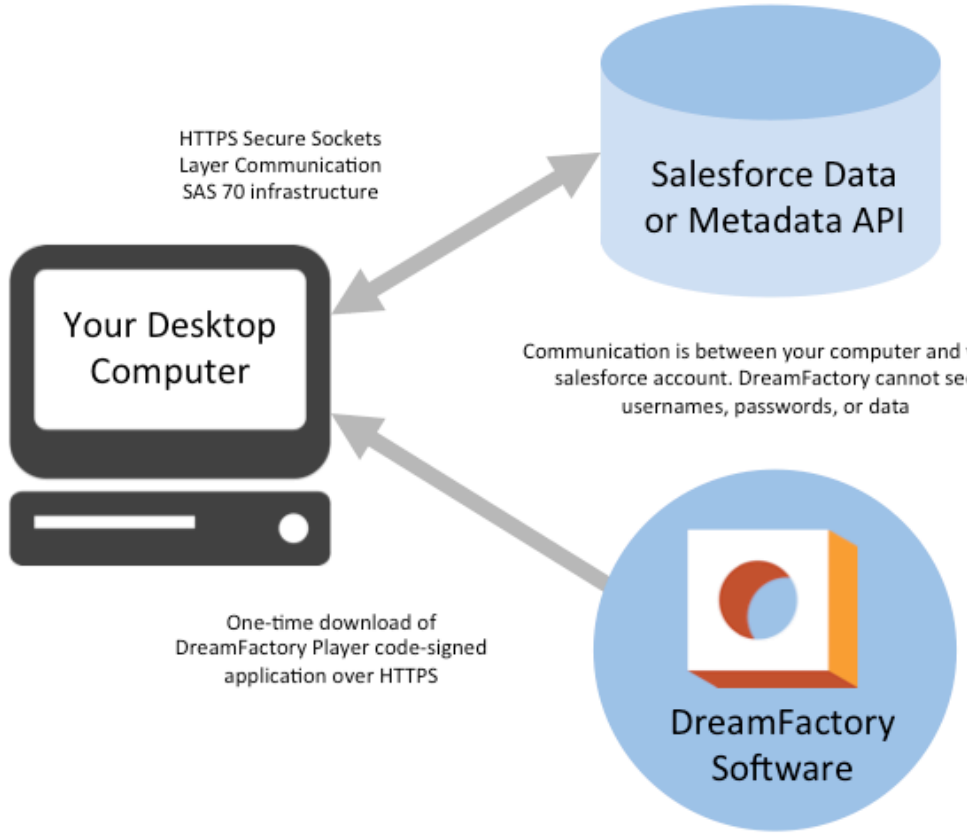

Figure 1: DreamFactory Security Architecture

The DreamFactory client operates in much the same manner as a web browser, but instead of communicating with HTML, we communicate with XML directly to the salesforce web services architecture. One advantage of this is the communication speed is greatly enhanced due to the direct connection, but another key advantage is that your data travels back and forth to salesforce directly and is not read by any other server. This strategy helps maximize customer security and privacy.

Salesforce Native Operation

DreamFactory applications use the salesforce.com Data or Metadata API, and so they are completely limited by the current account settings and visibility limitations as defined by the salesforce.com administrator. When a user logs into salesforce and navigates to a DreamFactory rich application, all the settings for that user are transferred through the session ID to the data accessed by that application. There is no way for a DreamFactory application to "see" things that the given user cannot otherwise see through the salesforce.com HTML or web services interface.

DreamFactory applications "sense" the current user settings for read, write, create, and delete of the various objects used by our applications. For example, a user

may be prompted that they do not have the ability to delete a certain object, and in other cases restricted objects simply do not show up at all for some users. Even if the user was somehow able to go forward and actually attempt to delete some protected object this would simply generate a runtime error message generated by the salesforce.com service architecture.

The Native Data Advantage

DreamFactory applications like DreamTeam store the data that they need in your salesforce.com account using appropriately named custom objects, similar to any other custom and standard objects in the salesforce system. There are many powerful advantages to storing this mission critical data directly in your salesforce.com account and not on someone else's server.

First, you don't have to depend on a potentially unreliable third party to store your data. Second, our applications take full advantage of all the existing data and other customizations that you have added to your salesforce.com account, including custom fields, integration links and custom objects. Lastly, all of the familiar salesforce.com services and interfaces work with the custom objects that our applications use to store their data, including reporting, dashboards, editing, linking, workflow, mobile access, offline access, and all other native capabilities of the salesforce.com platform.

DreamFactory Software Security Policy

The DreamFactory client enables your personal computer to communicate directly with your salesforce.com account. All transactions take place directly with salesforce.com and are conducted using the SSL protocol. All transactions conform to the AppExchange API security policy, and the policy that you have established for the users in your account. None of your private data or even your session ID is transmitted to us or to any other database. We never store your username or password. Our servers are only used for the initial download of the DreamFactory Player and salesforce product updates.

DreamFactory Software Privacy Policy

The DreamFactory Player enables your personal computer to communicate directly with your salesforce.com account. All of the data used by our salesforce products is stored in your account. None of your personal data is sent to us or stored on some other server. Any personal data that you explicitly send to us, for example to request product information, will be used solely for product licensing, customer relationships, and technical support. Your personal information will never be transferred to a third party or become linked to any database external to DreamFactory Software.

Appendix: Common Security Issues

What follows is a series of security issues that you should consider, and the approach DreamFactory takes in resolving these issues.

Issue 1: Protecting Data

Many AppExchange applications use JSP, ASP, Java, or some other server based technology to render HTML pages in the salesforce interface. In order to run the application, they must ship the current session ID back to their data center and access information in your account from there. While salesforce has a secure SAS 70 certified data center to deliver their service, most other partners do not. Where is their data center? What is their security policy? Who has access to your data? Is your data cached on their server? Which records are they reading with your session ID? What other databases do they have? What other servers are they connected to?

DreamFactory doesn't have a server. We aren't "hosting" anything. You download the desktop application from our web site and then you are done with us. Your private data is never shipped anywhere, except back and forth to salesforce.com through the encrypted SSL pipeline. We use the exact same HTTPS protocol that the browser does, except we read and write XML instead of HTML. Your private data, username, password, and session ID are not accessible to DreamFactory or some third party.

Issue 2: Protecting Credentials

When you log into salesforce.com a session ID is generated, and this ID is used by the service architecture to access your data. Shipping private data across the Internet is one thing, but server based solutions must also transfer your session ID to their data center. If your session ID is lost or stolen then any data visible to the current user can be read, updated, or even deleted. There is no way to know what account data has been accessed by a third party once they have your session ID, because these transactions take place behind their firewall. The potential for lost or stolen account data increases with every new server that has access to your session ID.

The DreamFactory Player only uses your session ID on your desktop computer to access your salesforce account. The session ID is used for communicating directly with salesforce.com, and then it is destroyed when our application terminates. The session ID is only used to access the data you request and then see moments later on your computer screen. Neither your private data nor your session ID is used for any other purpose. Please feel free to verify these claims and the secure behavior of our applications with a network monitor.

Contact Information

Author
Name: Bill Appleton
Email: billappleton@dreamfactory.com

Send an Email
Sales Questions: sales@dreamfactory.com
Partnership Program: partners@dreamfactory.com
Technical Support: techsupport@dreamfactory.com
Feature Requests: featurerequests@dreamfactory.com
Bug Reports: bugreports@dreamfactory.com
Web Site Problems: webmaster@dreamfactory.com

Company Location
DreamFactory Software, Inc.
1999 South Bascom Avenue, Suite 928
Campbell, CA 95008

Phone Numbers
Toll Free: 1-888-399-DREAM (3732)
Main: 1-650-641-1800
Fax: 1-650-898-1718

DreamFactory Websites:
https://www.dreamfactory.com (corporate website)
https://www.dreamfactory.net (product downloads)