Flosum Security Documentation

PURPOSE OF THIS DOCUMENT: 2
WHAT IS FLOSUM? 2
RELATIONSHIP BETWEEN SALESFORCE AND FLOSUM: 2
ARCHITECTURE: 2
SECURITY REVIEW: 3
HARDENING THE PLATFORM FURTHER: 3
USER PROVISIONING: 4
INTEGRATION WITH SINGLE SIGN-ON: 4
COMPLIANCE: 4
TRUST, AVAILABILITY, AND BUSINESS CONTINUITY PLANS: 4
CHANGE MANAGEMENT AND UPGRADE PROCESS: 4
DATA MANAGEMENT: 5
INCIDENT MANAGEMENT: 5
LOGGING AND MONITORING: 5
SYSTEM DEVELOPMENT LIFE CYCLE 5
APPENDIX: 6

PURPOSE OF THIS DOCUMENT:

The purpose of this document is to provide a brief overview of Flosum's approach to security. This document in written for security architects & experts who are responsible for evaluating this area of critical concern for application lifecycle management solutions (ALM) for their Salesforce environment.

WHAT IS FLOSUM?

Flosum is a complete Salesforce-based Application Lifecycle Management solution that is designed for the Salesforce.com platform. Flosum manages development processes from requirements planning all the way to deployment into production. As a native Salesforce.com application, Flosum promotes governance, compliance, and rapid innovation in the successful delivery of software.

RELATIONSHIP BETWEEN SALESFORCE AND FLOSUM:

Flosum has an OEM relationship with Salesforce. For every customer, Flosum procures a brand-new org (instance) with the relevant Salesforce licenses to run the Flosum application. This org can be created by the customer from Salesforce's marketplace (AppExchange).

All customers who procure Flosum already have access to Salesforce. All the security, data center, infrastructure, business continuity, disaster recovery, availability policies that are applicable to your existing Salesforce organization are also applicable to Flosum.

This new org is very similar to your existing production org that you have directly procured from Salesforce to run your business applications (such as Sales cloud, Service cloud, or your custom application).

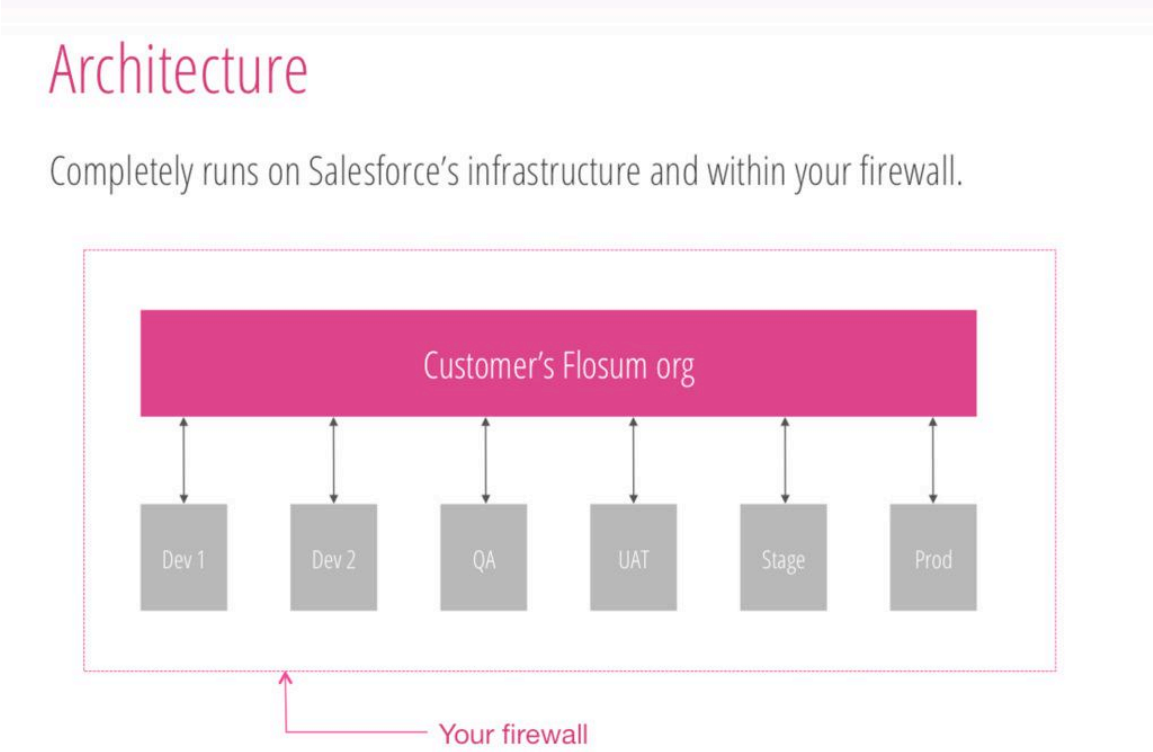
This new org is completely hosted by Salesforce and can be accessed only from your corporate network. This org cannot be accessed or modified by Flosum.

Physical security: The security treatment provided to your Flosum org is the same as Salesforce org.

ARCHITECTURE:

Flosum is only used by Salesforce customers. Customers who do not use Salesforce cannot use Flosum.

Flosum is completely built on Salesforce's Force.com platform. Flosum does not have any other servers or data center footprint. Flosum the company does not maintain any servers. The application is completely hosted by Salesforce. Customer can control who can access which pieces of data in the application. Flosum employees and personnel do not have any access to the application or the data within the application.



SECURITY REVIEW:

As a part of technical due diligence, most customers spend a lot of time in reviewing the security of the Salesforce platform. All the work done by a customer in reviewing the security of the Salesforce platform is also applicable to Flosum as a native application. This is because Flosum is completely built on the Salesforce platform and operating within the customer's Salesforce environment.

HARDENING THE PLATFORM FURTHER:

Flosum recommends leveraging the complete security best practices provided by Salesforce to further harden the security of the platform including the Flosum application.

USER PROVISIONING:

Since the Salesforce org is completely controlled by the customer, and Flosum personnel do not have access, the customer is responsible for provisioning new users within the application. User access management is completely controlled by the customer.

Password policy management is dictated by the Salesforce's policies and can be overridden by your single sign-on infrastructure.

INTEGRATION WITH SINGLE SIGN-ON:

Most customers have a corporate single sign-on directly, which stores the password for all the applications as well as provides the front-end interface to login into all applications at once. Customers can choose to integrate with their corporate single sign-on solution just the way they have done it for the production Salesforce instance.

COMPLIANCE:

Flosum is compliant with all the different certifications and compliances that are attested by the Salesforce platform including ISO 27001/27018, SSAE 16/ISAE 3402 SOC-1, SOC 2, SOC 3, PCI-DSS, TRUSTe Certified Privacy Seal, CSA STAR, and more.

TRUST, AVAILABILITY, AND BUSINESS CONTINUITY PLANS:

Flosum is completely built on the Salesforce platform; as such, the same SLAs for availability, business continuity, disaster recovery that apply to your production organization also apply to Flosum.

CHANGE MANAGEMENT AND UPGRADE PROCESS:

Flosum releases software upgrades three to six times a year. Some releases are minor, while other releases are major. Almost every release has new features and enhancements.

Here is how it works:

A Flosum Customer Success Director is in regular contact with the customer and will inform them about upcoming upgrades.

The new features are reviewed and discussed with each customer with every upgrade. If the customer sees enough business value in the new release, they can choose to upgrade.

At Flosum, upgrades are scheduled carefully so that it does not interfere with the customer's internal deployment schedules. Upgrades are only carried out with complete and due consent from the customer. Flosum recommends that you do not request upgrades two weeks before or after internal deployments.

Flosum does not upgrade its customers in the around the time of a Salesforce release. So, Flosum will not upgrade an org two weeks before or after a release from Salesforce.

DATA MANAGEMENT:

The data within the customer's application is completely hosted by and within Salesforce infrastructure. This is the same infrastructure used by the Salesforce production organization, which hosts the customer's Salesforce business application.

INCIDENT MANAGEMENT:

Flosum provides a dedicated support portal to manage any incidents experienced by customers. Customers create their own login and account and can create and submit any incidents encountered through the Flosum support portal.

LOGGING AND MONITORING:

Any policies or practices for logging and monitoring used in relation to a customer's Salesforce production organization are also applicable and used in conjunction to the Flosum organization.

SYSTEM DEVELOPMENT LIFE CYCLE:

In relation to ongoing development, enhancement and improvement of the Flosum application, Flosum leverages a comprehensive software development lifecycle.

Flosum uses Jira for capturing all the requirements from the Flosum product team. Flosum uses Zendesk for capturing incidents and new feature requests from customers. Flosum is internally used for its own application lifecycle management.

Flosum has very strong team of quality assurance engineers to ensure that the application is well tested.

MORE DOCUMENTATION:

Security implementation guide

Protecting your data in the cloud

Salesforce compliance

Security best practices