How Secure Is Your Salesforce Org?

Fortifying Salesforce With SnapShot Org Intelligence Reporting

DreamFactory White Paper

Ben Busse, VP Product Management
DreamFactory Software

The Challenges of Securing Your Salesforce Org

As an on-demand application, Salesforce enables companies to quickly deploy enterprise capabilities that increase productivity and facilitate end user collaboration. However, the very attributes that make the SaaS model attractive – centralized data, universal access, and rapid extensions – create a formidable challenge: how to provide the right information access and control policies that impact the lifeblood of your business.

There's a delicate balance between not enough employee access and too much access to your Salesforce Org. Insufficient access stifles collaboration, defeating a core benefit of investing in Salesforce in the first place. Too much access leaves you vulnerable to security gaps. These gaps become harder to identify as Salesforce is widely adopted in your company, new Org customizations evolve, users are added and removed, and Orgs are merged together.

Growth compounds the security challenge as each new custom object, field, or profile adds potential vulnerabilities that require oversight. Engaging third parties in your Salesforce deployments (consulting partners and Force.com applications) further complicates the security equation, requiring a sweeping strategy to mitigate risk.

Administrators need a comprehensive solution to secure their Salesforce implementation. This paper discusses how SnapShot's reporting and monitoring capabilities can help you fortify your Salesforce Org, including comprehensive control of:

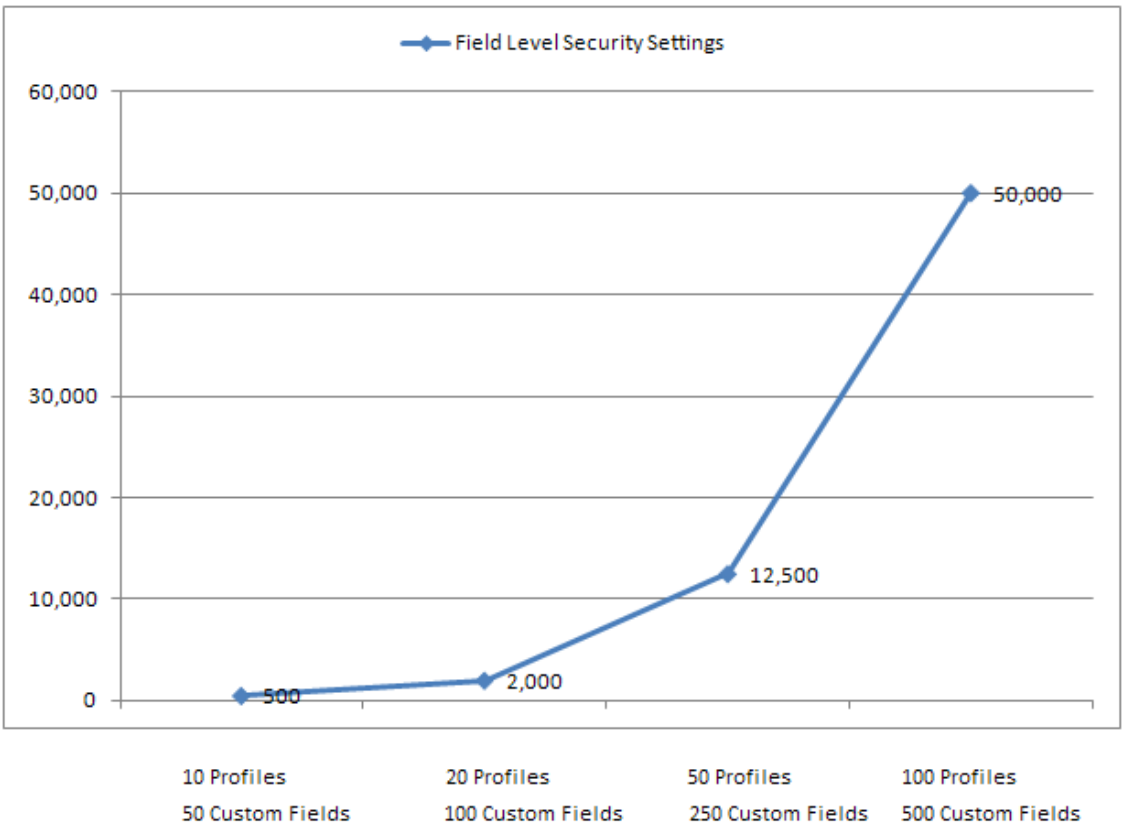
1) Access Rights
2) Customizations
3) Third-party extensions

Securing User Access Rights

When it comes to user access rights, Salesforce provides tremendous flexibility and fine-grained control. Administrators can set up any number of profiles and assign specific users to each profile. Each profile has its own access permissions and data visibility rights, including granular control over object permissions, field level security, and visibility to page layouts, custom applications, tabs, and record types.

With only a handful of profiles and a "vanilla" Salesforce configuration, managing all these profile settings and user assignments can be relatively straightforward at first. However, as soon as you start customizing Salesforce in any meaningful way, complexity explodes, resulting in the "n-squared" effect of managing the access rights of each profile multiplied by every type of permission setting (e.g., object permissions for each combination of profile and object, field level security for each combination of profile and field, etc.).

The chart below illustrates this non-linear growth effect using field level security as an example. The number of field level security settings grows as a function of both the number of profiles and the number of fields, quickly becoming too complex to manage without automation tools.



Furthermore, your Salesforce Org is rarely static. Shifting business requirements, organizational changes, and accelerating adoption of Salesforce inside your company guarantee that Salesforce customizations will keep evolving – schema changes to objects and fields, new page layouts and record types, the introduction of third-party applications and integrations, the merging of Orgs after company acquisitions and other organizational changes, and the continuing need to provision end users with appropriate security rights.

At any time, these questions should at the top of any Salesforce Administrator's mind:

- Which employees have access to which objects, fields, and record types? Has their access changed with the latest customization changes to our production Org?
- Which employees have access to which page layouts? Has their access changed with the latest customization changes to our production Org?
- Which employees have access to which permissions (e.g., modify all data, run reports, override forecasts, etc.)? Has their access changed with the latest customization changes to our production Org?
- Which employees are assigned to which profiles? Have these assignments changed with the latest customization changes to our production Org?

How do you efficiently answer all these questions? Each and every customization change introduces a potential security threat. To succeed, administering user access rights must be simple and repeatable.

Monitoring Customization Changes

A key benefit of implementing Salesforce is the ease of tailoring the application to meet your specific business needs. You don't have to be a programmer or IT expert to make basic customization changes. However, this degree of flexibility is a double-edged sword. The ease with which any Administrator can make configuration changes introduces a host of potential security vulnerabilities.

Many companies realize that monitoring changes to Salesforce is no different than monitoring changes to traditional mission-critical applications running behind a firewall – core business processes and critical information reside inside of Salesforce. The same change management rigor applied to on-premise applications and other business-critical applications also applies to SaaS-delivered solutions such as Salesforce. The underlying technology architectures may be different, but the nature of security threats introduced by application changes and the potential for end user abuse are no different.

The underlying challenge of monitoring and tracking changes to your production Org are compounded by more advanced customizations and the addition of multiple Salesforce Administrators, sometimes including temporary Admins from third-party consultants working on an implementation project. A small Salesforce Org with a single Administrator making simple, real-time production changes can likely get away without tracking every change or simply track changes by hand in a spreadsheet.

On the other hand, any Salesforce customer with multiple Salesforce Admins, a structured deployment process of "pushing" changes between development, sandbox and production Orgs, and many interdependent customizations – significant object and field customizations, user interface customizations with page layouts, and the use of multiple custom profiles – needs to know which Salesforce Administrator made customization changes to production, when those changes were made, and exactly what changes occurred.

Each and every customization change introduces a potential security threat. To mitigate risk, you must be able to quickly answer these key questions and roll back changes if necessary.

- Which Administrators have made customization changes?
- Exactly what did they change?
- When did they change it?

Securing Third-Party Customizations and Applications

Another great benefit of using Salesforce is the opportunity to extend the application in different ways. You can integrate Salesforce with other SaaS applications and with other on-premise applications. You can install numerous third-party applications from the AppExchange that run directly inside of Salesforce's user interface or build your own custom applications that run natively on Force.com.

Companies commonly hire third-party consultants and systems integrators to customize Salesforce, particularly in cases where a fair amount of expertise is required to tailor Salesforce to meet specific business requirements or to build advanced connectors between other IT systems. External consultants usually provide some detailed

documentation of the customization work they've performed, often based on a business requirements document.

However, without a comprehensive record of specific customization changes to your Salesforce Org, you're at a loss for details about what actually occurred (for example what objects and fields changed, what workflow rules changed, which profile permissions changed, what Apex code was added, etc.) and how these specific changes might impact future deployments. Worse yet, you have no idea about the security implications of changes made by external parties. How have all of these changes affected existing user access rights? Is your Org sufficiently secure after all these changes?

Adding third-party applications from the AppExchange or building your own applications on Force.com adds another level of security complexity, particularly when the information stored in these applications is sensitive. Each application has its own set of objects and fields, tabs, and page layouts and each user profile has specific access rights to each of these application assets. Managing all these access rights across many user profiles takes significant time and diligence, but is nonetheless essential to security.

Hiring third-party consultants and adding third-party applications to Salesforce poses a significant security challenge. To mitigate risk, you should always be prepared to answer the key questions below and roll back changes if necessary.

- After an external consultant has completed a project, exactly what aspects of our production Org did they change? How do user access rights after the project compare to before the project?
- Which employees have access to which applications? Has their access changed with the latest customization changes to our production Org?

SnapShot – Fortifying Your Salesforce Org

The challenges of managing Salesforce security are big and DreamFactory has developed a solution called SnapShot to help.

SnapShot is the leading Change and Release Management environment for Salesforce, designed from the ground up to help companies manage the numerous security challenges described in this paper. SnapShot provides:

- Before and after snapshots of every customization setting in a Salesforce Org
- One place to run detailed reports covering each and every security setting in Salesforce
- Ability to compare security settings before and after a deployment to see precisely what security settings have changed
- Ability to easily monitor and track customization changes to see exactly what changes were made, when it happened, and who was responsible

Comprehensive Org Security Reporting

SnapShot enables Salesforce Administrators to take a “snapshot” of a Salesforce Org. SnapShot uses the Salesforce metadata API to query all customization settings in your Org (metadata such as objects, fields, page layouts, profiles, applications, tabs, etc.) and saves these settings as a viewable document called a snapshot.

Once you’ve taken a snapshot, you can browse, navigate, and report on all the details of your Salesforce customization within the SnapShot application. You can also compare snapshots taken at different points in time in the same Org or in different Orgs (for example a snapshot of a sandbox org compared to a snapshot of a production Org) to see exactly how the security settings differ.

SnapShot provides a comprehensive set of security reports that cover every important aspect of Salesforce security, including the following settings for each user profile:

- Object permissions
- Field level security
- Page layout assignments
- Application visibility
- Tab visibility
- Record type visibility
- Profile permissions
- User assignments to profiles

Object Permissions	Case	Collateral	Object Permissions	Case
			Authenticated Website	No Access
Contract Manager	Allow Create, Read and Edit	Allow Crea	Contract Manager	Allow Create, Read and Edit
Custom Apex User	No Access	Allow Crea		
Custom Profile	Allow Create, Read, Edit and Delete	Allow Crea		
Custom: Support VP Profile	Allow Create, Read, Edit and Delete	Allow Crea		
Custom: Cannot Delete	Allow Create, Read and Edit	Allow Crea		
Custom: Channel Manager	Allow Create, Read and Edit	Allow I		
Custom: Marketing Profile	Allow Read	Allow Crea	Custom: Marketing Profile	Allow Create, Read and Edit
Custom: Partner	Allow Read			
Custom: qsadmin	Allow Create, Read, Edit and Delete	Allow Crea		
Custom: Sales Profile	Allow Read	Allow Crea	Custom: Sales Profile	Allow Create, Read and Edit
Custom: Sales VP Profile	Allow Read	Allow Crea		
Custom: Support Profile	Allow Create, Read, Edit and Delete	Allow Crea	Custom: Support Profile	Allow Create, Read, Edit and Delete
Custom: Top Executive	Allow Create, Read and Edit	Allow Crea		
			Customer Portal Manager	Allow Create, Read and Edit
			DreamFactory Dev Test Profile	No Access
			Force.com - Free User	No Access
Gold Partner	Allow Create, Read and Edit			
			High Volume Customer Portal	Allow Create, Read and Edit
Marketing User	Allow Create, Read and Edit	Allow Crea	Marketing User	Allow Create, Read and Edit
Partner User	Allow Create, Read and Edit		Partner User	Allow Create, Read and Edit
Read Only	Allow Read		Read Only	Allow Read
			Service Cloud	Allow Create, Read, Edit and Delete
Solution Manager	Allow Create, Read and Edit	Allow Crea	Solution Manager	Allow Create, Read and Edit

SnapShot's Org security reporting enables you to efficiently answer all user access questions described earlier:

- Which employees have access to which objects, fields, page layouts, records types, and tabs?
- Which employees have access to which custom applications?
- Which employees have access to modify all data, run reports, override forecasts, and numerous other permission settings?
- Which employees are assigned to which profiles?
- After an external consultant has completed a project, exactly what aspects of our production Org did they change?
- How has employee access changed with the latest customization changes to our production Org?

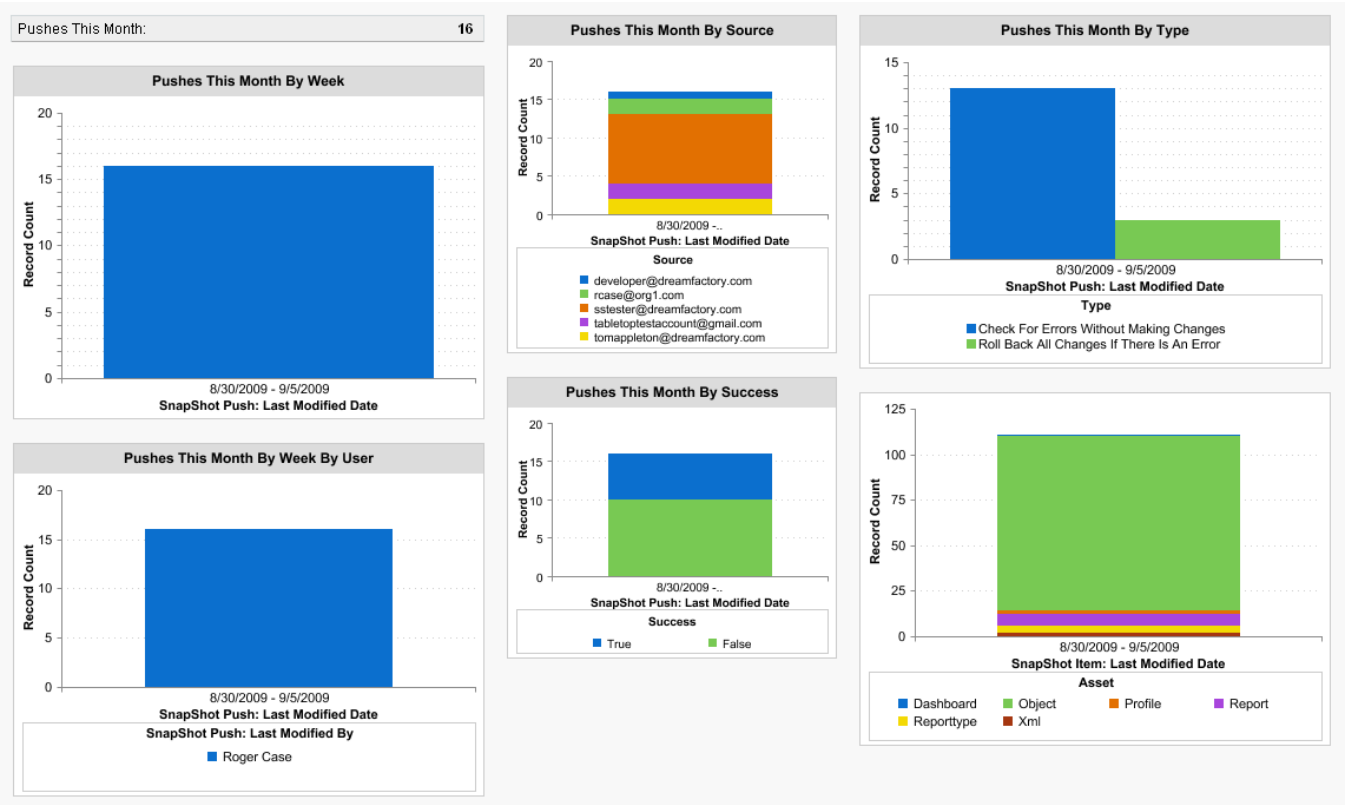
To streamline security assessments, a company using SnapShot will typically follow these steps each time changes are made to a sandbox or production Org:

1. Take a snapshot immediately before a deployment
2. Deploy customizations using SnapShot's push feature
3. Take a snapshot immediately after the deployment
4. Run "before" and "after" snapshot reports on each area of security configuration to isolate every change, from object permissions to the assignment of users to profiles
5. Save both the "before" and "after" snapshots as a historical record of each and every security change
6. If any security vulnerabilities are discovered, roll back to the security settings documented in the "before" snapshot

Change Management Command Center

In addition to providing detailed reporting on user access rights, SnapShot provides key insight on deployment events that can affect Org security. The SnapShot Logger tells you which Administrator has pushed out a set of customization changes, exactly what changes were deployed, and precisely when the changes were released to a sandbox or production Org.

Every time an Administrator pushes changes between Orgs, this information is logged and stored in a custom object, allowing you to view each logged event with Salesforce reports and dashboards that come packaged with SnapShot. You can also configure Salesforce's Chatter feed to follow the SnapShot Logger custom object – an easy way to track all this deployment information as it happens in real time.



From a security standpoint, SnapShot Logger provides a detailed trail of every single change ever made to your production Org. If security gaps are suddenly introduced by a configuration mistake, you can quickly identify what was changed, determine who deployed the changes, and roll back the changes if necessary.

About DreamFactory

DreamFactory Software is the world's leading publisher of rich web applications for cloud platforms. Our products combine the agility of on demand delivery with the performance of desktop applications. The DreamFactory Suite delivers enterprise class project, document, and data collaboration software to over 7,000 businesses using Force.com, Amazon Web Services, Intuit Partner Platform, Cisco Connect, and Windows Azure.

Additional Resources

For more information about SnapShot, please contact DreamFactory at sales@dreamfactory.com or visit our website at www.dreamfactory.com.