

Snapshot Use Cases: Compliance, Governance, and Security

Introduction

Many large companies have established policies for corporate governance. Others follow security policies to safeguard consumer or financial information. Companies in the financial and health sectors are regulated by state, federal, and foreign governments. Various regulations include SOX, PCI-DSS, GLBA, HIPAA, HCQIA, CHIP, HRRP, PSQIA, ACA, FISMA, PCI-DSS, FERPA, and most recently GDPR. Regulatory compliance requires careful documentation of corporate activities and information handling practices. This whitepaper discusses how the Snapshot 2.0 Change and Release Management product from Metazoa can help companies achieve better compliance, governance, and security.

Data Dictionary

Custom Objects and Fields are a central focus for any Salesforce account. Between the Data and the Metadata API, there are 70 properties that describe Custom Objects. There are another 80 properties that document Custom Fields. These properties cover everything you can imagine, such as field labels, numeric precision, formula fields, date formats, picklist values, child relationships, and help text.

The Snapshot Data Dictionary can be used to document the current properties for each Custom Object and Field in a Salesforce account. This is a key compliance report for use by business analysts and application developers interested in documenting the current state of the org. The report could be used by a development team to track project progress, or by a System Integrator before and after a job is completed. This report is useful for compliance and governance.

Combined Security Report

Every user has a Profile that defines what they can see and do. Profile permissions include Application and Tab Visibility, Apex Class and Page Access, Object and Field Permissions, User and Custom Permissions, and Layout Assignments. An administrator can also assign any number of Permission Sets to a user. Permission Sets are similar to Profiles. They are used to grant additional permissions for special situations.

The Snapshot Profiles and Permission Sets dialog includes a Combined Security Report that shows how the base Profile and each assigned Permission Set contribute to the actual security permissions for selected users. This is a key report for security and compliance. For example, a company could document which users have been granted access to fields that contain customer information. In the table below, Permission Sets that changed the base Profile are shown in green, Permission Sets that were not effective are shown in red.

Combined Security Vs Object Permissions

Object Permissions	A_DX_Object__c	Account
tester@metazoa.com (Doug Martin)	Customer Portal Manager Custom (No Access) Combined Security (No Access)	Customer Portal Manager Custom (Create, Edit, Read) Combined Security (Create, Edit, Read)
joshdev@metazoa.com (Josh Hyde)	Custom: Standard User (No Access) Combined Security (No Access)	Custom: Standard User (No Access) Set_User_Perm (Read) Account_Object_Manipulation (Create, Read) Account_Object_Manipulation_2 (Delete, Edit, Read) Combined Security (Create, Delete, Edit, Read)
newss@df.com (Bill Smith)	Admin (No Access) Account_RW (Create, Delete, Edit, Read) Combined Security (Create, Delete, Edit, Read)	Admin (Full Access) Opportunity_RW (Full Access) Account_RW (Full Access) Combined Security (Full Access)

Record Level Security Report

Profiles and Permission Sets control which objects and fields a user can see. But when it comes to specific records, additional rules apply. Salesforce administrators can set up complex record level security rules. Every record is owned by a user or a queue. The owner has full access to the record. There are organization-wide sharing settings for each object. Users higher up in the Role hierarchy have access to the same data as people lower in their hierarchy. Lastly, manual and programmatic sharing rules create exceptions for particular sets of users.

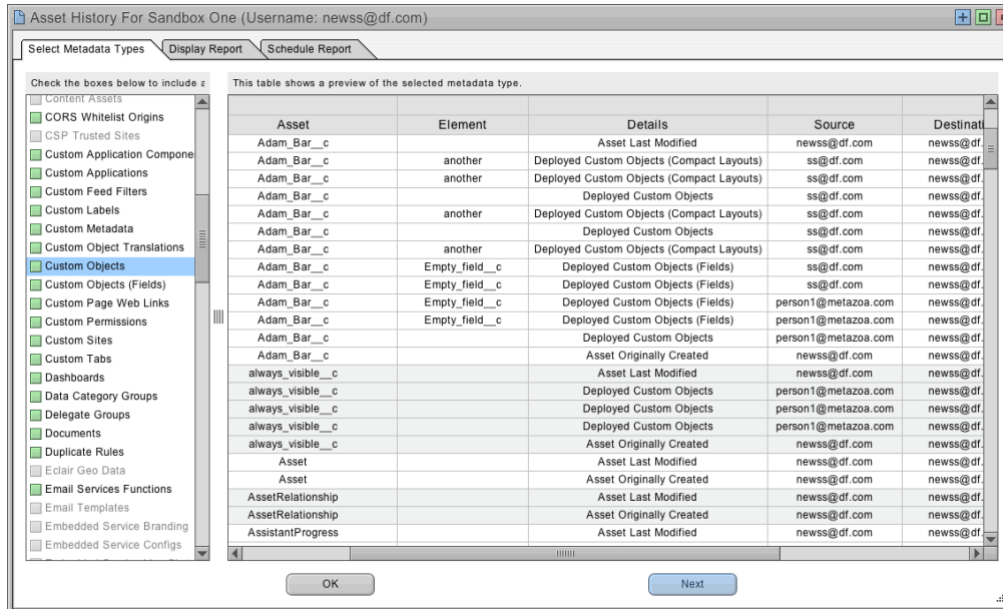
There is some information on record level access in the Salesforce HTML interface, but only for one record at a time. The Snapshot Record Level Security Report allows any set of records to be selected and then provides detailed information about who has access to each record, what kind of access they have, and why they have the access. This report can help administrators manage sharing rules and document data security.

Asset History Report

Think for a second about your production Salesforce account. Most orgs will have Custom Tabs, Page Layouts, Custom Objects, Profiles, Visualforce Pages, and many other configurations. The Metadata API currently supports about 150 different types. And for each type, there are many individual assets. An Unlimited Edition org can have up to 2000 Custom Objects, each with a maximum of 500 fields. There can be hundreds or even thousands of Roles, Profiles, Dashboards, and other assets.

Now think about this. Where did all those configurations come from? Who deployed them in the org? Did they flow through the testing Sandbox? Were they modified with the Setup Menu? What was the chain of custody from the developer who created the asset down through various Sandboxes and other staging orgs before it ended up in your production account?

The Snapshot Asset History Report can answer these questions. This report mines the “meta metadata” that Snapshot stores in the licensed org along with additional information from the Salesforce Metadata, Tooling, and Data API. As a result, the Asset History Report can tell you *where* each metadata asset was originally created, *what* changes were made to the asset, *who* made these changes, *which* orgs the asset moved through, and *when* the asset was last modified. This is a game-changing report for compliance, security, and governance.



Asset History For Sandbox One (Username: newss@df.com)

Select Metadata Types | Display Report | Schedule Report

Check the boxes below to include:

- Content Assets
- CORS Whitelist Origins
- CSP Trusted Sites
- Custom Application Components
- Custom Applications
- Custom Feed Filters
- Custom Labels
- Custom Metadata
- Custom Object Translations
- Custom Objects
- Custom Objects (Fields)
- Custom Page Web Links
- Custom Permissions
- Custom Sites
- Custom Tabs
- Dashboards
- Data Category Groups
- Delegate Groups
- Documents
- Duplicate Rules
- Eclair Geo Data
- Email Services Functions
- Email Templates
- Embedded Service Branding
- Embedded Service Configs

This table shows a preview of the selected metadata type.

Asset	Element	Details	Source	Destination
Adam_Bar_c		Asset Last Modified	newss@df.com	newss@df.com
Adam_Bar_c	another	Deployed Custom Objects (Compact Layouts)	ss@df.com	newss@df.com
Adam_Bar_c	another	Deployed Custom Objects (Compact Layouts)	ss@df.com	newss@df.com
Adam_Bar_c		Deployed Custom Objects	ss@df.com	newss@df.com
Adam_Bar_c	another	Deployed Custom Objects (Compact Layouts)	ss@df.com	newss@df.com
Adam_Bar_c		Deployed Custom Objects	ss@df.com	newss@df.com
Adam_Bar_c	another	Deployed Custom Objects (Compact Layouts)	ss@df.com	newss@df.com
Adam_Bar_c	Empty_field_c	Deployed Custom Objects (Fields)	ss@df.com	newss@df.com
Adam_Bar_c	Empty_field_c	Deployed Custom Objects (Fields)	ss@df.com	newss@df.com
Adam_Bar_c	Empty_field_c	Deployed Custom Objects (Fields)	person1@metazoa.com	newss@df.com
Adam_Bar_c	Empty_field_c	Deployed Custom Objects (Fields)	person1@metazoa.com	newss@df.com
Adam_Bar_c		Deployed Custom Objects	person1@metazoa.com	newss@df.com
Adam_Bar_c		Asset Originally Created	newss@df.com	newss@df.com
always_visible_c		Asset Last Modified	newss@df.com	newss@df.com
always_visible_c		Deployed Custom Objects	person1@metazoa.com	newss@df.com
always_visible_c		Deployed Custom Objects	person1@metazoa.com	newss@df.com
always_visible_c		Deployed Custom Objects	person1@metazoa.com	newss@df.com
always_visible_c		Deployed Custom Objects	person1@metazoa.com	newss@df.com
always_visible_c		Asset Originally Created	newss@df.com	newss@df.com
Asset		Asset Last Modified	newss@df.com	newss@df.com
Asset		Asset Originally Created	newss@df.com	newss@df.com
AssetRelationship		Asset Last Modified	newss@df.com	newss@df.com
AssetRelationship		Asset Originally Created	newss@df.com	newss@df.com
AssistantProgress		Asset Last Modified	newss@df.com	newss@df.com

OK Next

Metadata Differences Report

The Asset History Report looks at how the metadata assets in your Salesforce org were assembled, but additional insights can be gathered by watching how the org has changed over time. The Manage Time-Series dialog provide a Metadata Differences Report that can show the changes over time between any two snapshots. Have Profiles or Permission Sets changed? What new Custom Fields have been added? Did the security configuration change? Have new packages been installed? What Apex Scripts were changed? The Metadata Differences Report provides valuable information for security audits and compliance.

User Activity Timeline Report

The User Activity Timeline report shows all of the activities that a given user performed during a specified time frame. This report mines information from many different Salesforce objects and systems in order to paint a complete picture of user activity. This information can be used to monitor user activities and trigger alerts if problems are detected, or the report can be used forensically to investigate an incident in the past for security or governance purposes. The User Activity Timeline report is a key security capability for any Salesforce org.

In the event of a credential-based attack, this report can provide a roadmap of the activities carried out by the attacker. In a data exfiltration event, this report can be used to document the extent of the damage. Rogue administrative actions or accidents can be placed on a timeline. Different activities can be filtered by risk level. The Activity Timeline Report can be used to forensically examine events in the past, or proactively safeguard against future security risks.

newss@df.com	From 5/6/2018	To 5/21/2018		
Object Type	Object Name	Activity Date	Risk Level	Activity Details
LoginHistory	Invalid Password	5/7/2018 8:32 AM	MEDIUM_RISK	Application=Apex Plugin, ApiType=SOAP Partner, ApiVersion=42.0, Browser=I
SetupAuditTrail	DataManagement	5/7/2018 12:05 PM	MEDIUM_RISK	Display=Emptied 536 record(s) from the Recycle Bin
SetupAuditTrail	CustomObjects	5/8/2018 1:13 PM	LOW_RISK	Display=Created custom field Extra Field (Text Area) on DreamFactory Shared
SetupAuditTrail	CustomTabs	5/11/2018 3:45 PM	LOW_RISK	Display=Changed style of Adam Bars custom object tab from Car to Jewel
SetupAuditTrail	WorkflowRule	5/12/2018 10:53 AM	LOW_RISK	Display=Deleted Task Pending Close for Object: Opportunity
SetupAuditTrail	CustomizeAccounts	5/15/2018 12:22 PM	MEDIUM_RISK	Display=Created custom formula field: Custom Record ID (Text)
Adam_Bar__c	Freddy	5/16/2018 2:46 PM	LOW_RISK	Created Adam_Bar__c=Freddy
SetupAuditTrail	ManageUsers	5/16/2018 4:22 PM	HIGH_RISK	Display=Changed profile for user Josh Hyde from Custom: Standard User to C
EventLogFile	MetadataApiOperation	5/17/2018 5:00 PM	MEDIUM_RISK	OPERATION=meta_list, CLIENT_IP=71.204.191.46
EventLogFile	TransactionSecurity	5/17/2018 5:00 PM	MEDIUM_RISK	RESULT=TRIGGERED, EVALUATION_TIME_MS=214.0
EventLogFile	URI	5/17/2018 5:00 PM	LOW_RISK	REQUEST_STATUS=R, CLIENT_IP=73.71.153.152
EventLogFile	Login	5/17/2018 5:00 PM	LOW_RISK	BROWSER_TYPE=Metazoa, CLIENT_IP=73.71.153.152, LOGIN_STATUS=L
EventLogFile	ApexExecution	5/17/2018 5:00 PM	LOW_RISK	NUMBER_SOQL_QUERIES=3, ENTRY_POINT=TxnSecurityPolicyCondition
EventLogFile	Logout	5/17/2018 5:00 PM	LOW_RISK	USER_TYPE=S, SESSION_TYPE=A, SESSION_LEVEL=1, USER_INITIATED

Compliance, Governance, and Security

Companies can use Snapshot to generate powerful reports that help achieve better compliance, governance, and security. Let us know if we can help you improve compliance, governance, and security at your company.

support@metazoa.com

1-833-METAZOA

1-833-638-2962

<https://www.metazoa.com>

Twitter: @metazoa4sf

Facebook: <https://www.facebook.com/metazoa4sf>

LinkedIn: <https://www.linkedin.com/company/18493594/>