



Qualys SaaS Detection and Response (SaaS DR)

Release Notes

Version 1.6.0

April 12, 2022

Here's what's new in SaaS Detection and Response 1.6.0!

[Fixing Security Misconfigurations on Office 365 Tenants](#)

[New Home Page](#)

[Unified Dashboard \(UD\) Support for SaaS DR](#)

[Control Evaluation and Evidence at Resource Level](#)

[Improved View of Events Data](#)

[Content Updates](#)

Fixing Security Misconfigurations on Office 365 Tenants

The compliance assessment marks specific controls (checks) as failed if corresponding configurations are not hardened enough. To fix such misconfigurations, Office 365 administrators need to log in to the Office 365 admin center.

With this release, Qualys introduces a new auto-remediation feature in SaaS DR that allows you to fix the misconfigurations right from the SaaS DR UI without having to separately log in to the Admin Center of Office 365.

Note: You can only fix tenant-level misconfigurations without logging into the Office 365 admin center.

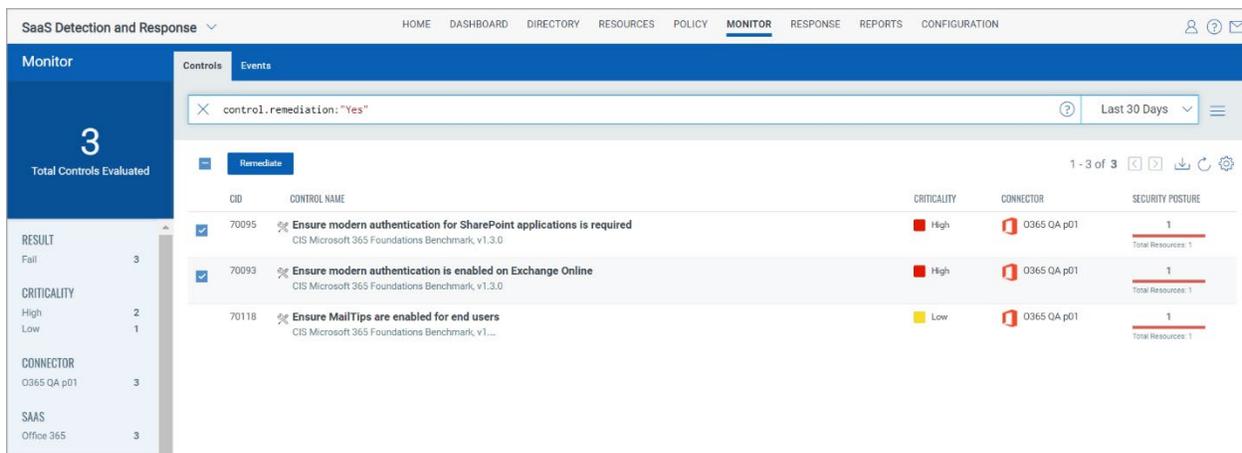
To filter the tenant-level misconfiguration, use the **control.remediation: "Yes"** search token. It filters and displays only those failing controls and thus is remediable.

The connector through which the remediation is performed must have the following privileges and roles:

- Enable the following App Permissions:
 - Exchange Administrator
 - SharePoint administrator
- Grant the following User Roles/Permissions:
 - Teams Administrator
 - Privileged Role Administrator

To remediate a control, go to the **Monitor > Controls** tab, select the control(s) you want to remediate, and click **Remediate**.

Note: Only the controls with an  icon are remediable. Use the **control.remediation: "Yes"** search token to filter the remediable controls.



The screenshot shows the SaaS Detection and Response interface. The top navigation bar includes HOME, DASHBOARD, DIRECTORY, RESOURCES, POLICY, MONITOR (selected), RESPONSE, REPORTS, and CONFIGURATION. The main content area is titled "Monitor" and shows a search filter "control.remediation: 'Yes'" and a "Remediate" button. A table lists three failed controls:

CID	CONTROL NAME	CRITICALITY	CONNECTOR	SECURITY POSTURE
70095	Ensure modern authentication for SharePoint applications is required CIS Microsoft 365 Foundations Benchmark, v1.3.0	High	O365 QA p01	1 Total Resources: 1
70093	Ensure modern authentication is enabled on Exchange Online CIS Microsoft 365 Foundations Benchmark, v1.3.0	High	O365 QA p01	1 Total Resources: 1
70118	Ensure MailTips are enabled for end users CIS Microsoft 365 Foundations Benchmark, v1.3.0	Low	O365 QA p01	1 Total Resources: 1

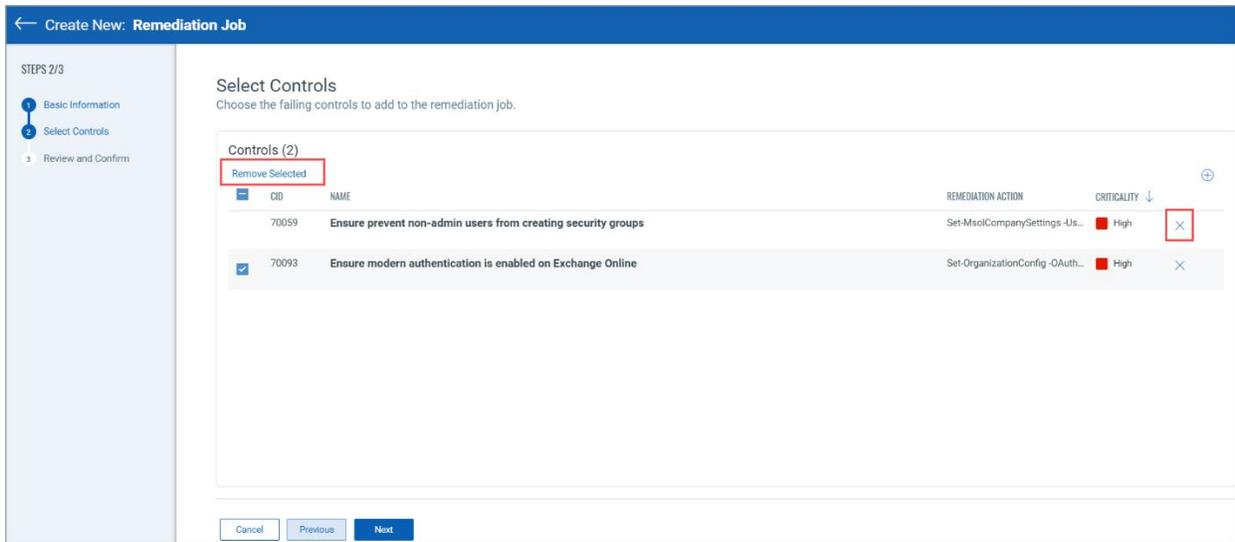
Creating a Remediation Job

Once you click **Remediate**, you can create a remediation job.

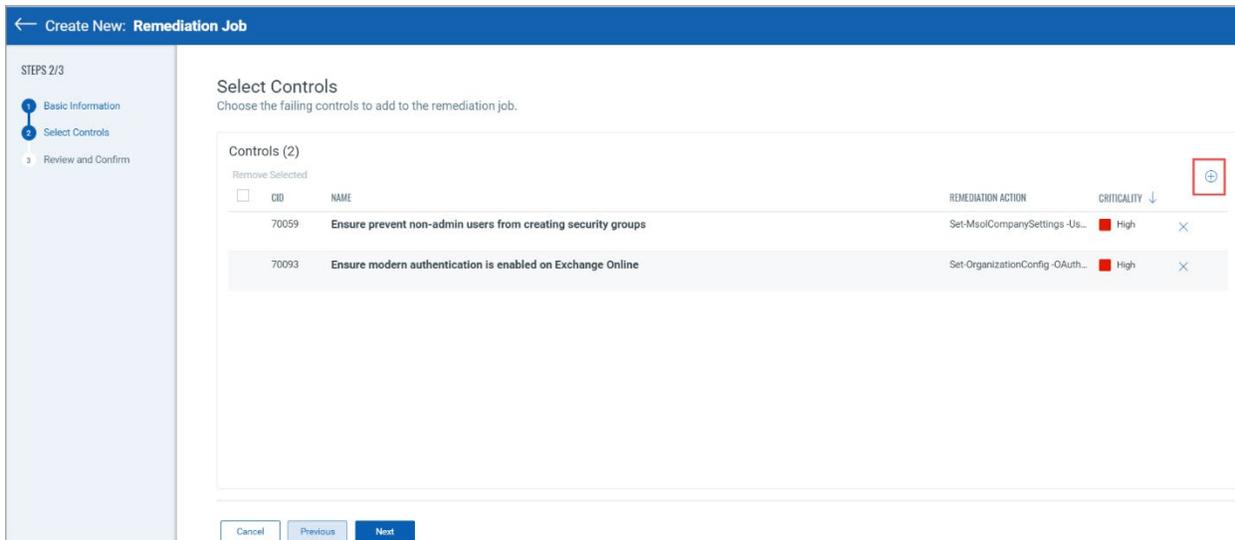
1. On the Basic Information window, enter the **Name** and **Description** and click Next. The SaaS and the Connector fields are auto-populated.
2. On the Select Controls window, click **Next** if all the details appear correctly.
Or,

Optional: You can choose to remove controls or add new controls.

Remove controls: Select one or more controls available in the list and click **Remove Selected** or use the Remove control icon to remove control.



Add controls: You can also add controls when creating the remediation job using the **Add Controls** icon as highlighted below:



3. Review the controls and click **Next**.

- On the Review and Confirm window, confirm the details and click **Create**.

The screenshot shows the 'Create New: Remediation Job' window in the 'Review and Confirm' step. The left sidebar shows three steps: 1. Basic Information, 2. Select Controls, and 3. Review and Confirm. The main content area is titled 'Review and Confirm' and includes a sub-header 'You're all done! Review your selection and click Submit. This remediation job will be created and added to your remediation jobs list.'

Basic Information

Name	test	Description	-
SaaS	Office 365	Connector	O365 2103

Selected Controls

CID	NAME	REMEDIATION ACTION	CRITICALITY ↓
70059	Ensure prevent non-admin users from creating security groups	Set-MsolCompanySettings -Us...	High
70093	Ensure modern authentication is enabled on Exchange Online	Set-OrganizationConfig -OAuth...	High

Buttons: Cancel, Previous, Create

Once you initiate the remediation, the compliance scan automatically reflects the latest compliance posture. The status of the controls changes based on the scan results once the remediation is successful.

View Status of the Controls

To check the status of the controls, go to the **Monitor > Controls** tab.

In the **Response** tab, you can view the status of different response activities and export the details if required.

In the **Remediation Jobs** sub-tab, you can check the remediation jobs used to fix the misconfigurations on your SaaS tenants.

The screenshot shows the 'SaaS Detection and Response' interface. The top navigation bar includes: HOME, DASHBOARD, DIRECTORY, RESOURCES, POLICY, MONITOR, **RESPONSE**, REPORTS, CONFIGURATION. The left sidebar shows 'Response' with a '1 Total Remediation Jobs' indicator. The main content area is titled 'Remediation Jobs' and includes a search bar, an 'Enable' button, and a table with the following data:

NAME	STATUS	CONNECTOR	CREATED BY	NUMBER OF CONTROLS COMPLETED
Remediate control	Disabled	O365_1	[Redacted]	0 of 1

Additional details: 1 - 1 of 1, [Navigation icons], [Settings icon]

STATUS: Disabled 1
OWNER: [Redacted] 1

Note: The remediation job needs to be explicitly enabled to get it started.

New Home Page

The SaaS DR 1.6 release comes with a modified **Home** page.

On the Home page, the three sub-tabs give you in-depth knowledge of the supported features.

Build Inventory

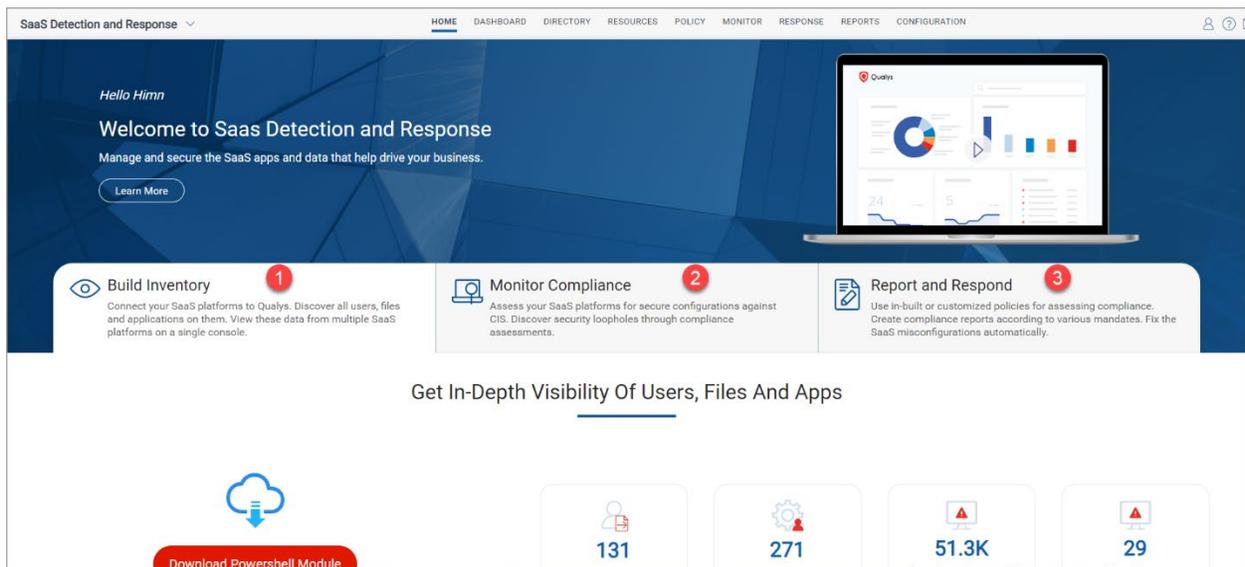
View all the Users and User Groups in your organization. Also, view all your resources, like files and folders, third-party applications, and meetings identified from the scanned SaaS applications.

Monitor Compliance

Enable and run the CIS Microsoft 365 Foundations Benchmark v1.3 policy for your connectors. View the policy controls to monitor your compliance posture.

Report and Respond

Perform different actions on the existing reports. Fix the security misconfigurations in SaaS to enhance their security posture.

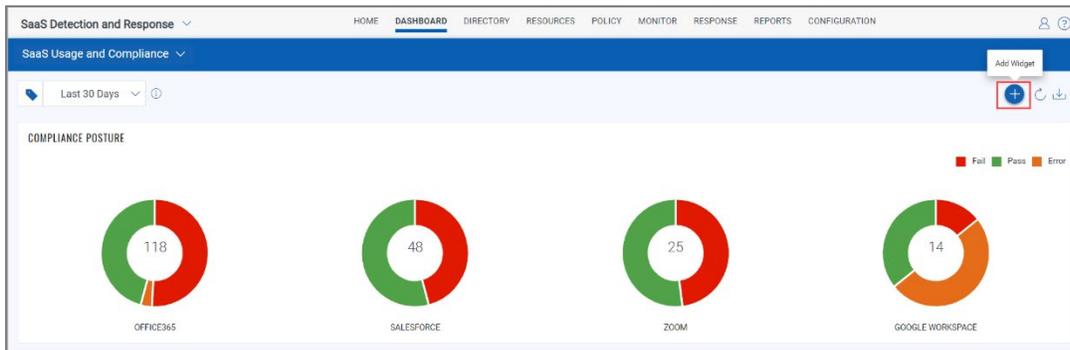


Unified Dashboard (UD) Support for SaaS DR

Dashboards help you visualize your resources such as assets, users, and applications, see your threat exposure, vulnerabilities, misconfigurations, and highlight essential findings in a summarized manner. We have integrated Unified Dashboard (UD) with SaaS Detection and Response (SaaS DR).

UD brings information from all Qualys applications into a single place for visualization. UD provides a robust new dashboarding framework and a platform service used by all other products to enhance the existing dashboard capabilities. You can use the default dashboard provided by Qualys or easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your vulnerability posture view.

Click the **Add Widget** icon on the Dashboard page to access the **Add Widget to Dashboard (SaaS DR)** screen to add more widgets.



Control Evaluation and Evidence at Resource Level

You can now view the control evaluation and evidence details at the resource level instead of the policy level. Go to **Monitor > Controls** and click the Security Posture of the control for which you want to view the evaluation and evidence details.

Under the Evidence column, click **Show Details** to view the evaluation details.

The screenshot shows the 'Control Evaluation' page for 'CID-70104 Ensure DLP policies are enabled'. The policy is 'CIS Microsoft 365 Foundations Benchmark, v1.3.0', last evaluated on 'Feb 3, 2022 04:18 PM', and has a 'High' criticality. The interface includes a search bar, a date filter set to 'Last 30 Days', and a table with 3 items. The table has columns for 'RESOURCE', 'EVALUATED ON', 'RESULT', and 'EVIDENCE'. The third row, 'Canada Personal Health Information Act (PHIA) - Manitoba', is highlighted in red and has a red box around its 'Show Details' link.

RESOURCE	EVALUATED ON	RESULT	EVIDENCE
Saudi Arabia - Anti-Cyber Crime Law	Feb 3, 2022 04:18 PM	PASS	Show Details
Australia Financial Data	Feb 3, 2022 04:18 PM	PASS	Show Details
Canada Personal Health Information Act (PHIA) - Manitoba	Feb 3, 2022 04:18 PM	FAIL	Show Details

You can view the evaluation details with Pass/Fail reasons.

This screenshot shows the 'Evidence Details' for the failed resource 'Canada Personal Health Information Act (PHIA) - Manitoba'. The details are displayed in a light gray box with a red border. The text reads: 'DLP Policies are set to: TestWithoutNotifications'.

Evidence Details

DLP Policies are set to: TestWithoutNotifications

Improved View of Events Data

You can view all types of connectors' events under the **Severity** column introduced with this release under the Monitor > Events sub-tab.

The **IP** and **Result** columns are now removed from the grid but not from metadata. You can still view the IP and Results in the metadata details.

New filters are also added for **Category**, **Sub-category**, and **Severity**.

The screenshot shows the 'Monitor' section of the SaaS Detection and Response interface. The 'Events' sub-tab is active, displaying a table of 1728 events. The table has columns for NAME, CONNECTOR, TIME, ACTOR, and SEVERITY. The SEVERITY column is highlighted with a red box. The left sidebar shows filters for CATEGORY, SUB CATEGORY, and SEVERITY.

NAME	CONNECTOR	TIME	ACTOR	SEVERITY
Add owner to group	Office365 P26	Jan 6, 2022 02:12 PM	Microsoft Teams Services	LOW
Add member to role	Office365 P26	Jan 6, 2022 02:08 PM	mjosshi@QualysSSCMSDev.com	LOW
Add member to role	Office365 P26	Jan 6, 2022 02:07 PM	mjosshi@QualysSSCMSDev.com	LOW
Add member to role	Office365 P26	Jan 6, 2022 02:04 PM	mjosshi@QualysSSCMSDev.com	LOW
UserLoggedIn	Office365 P26	Jan 6, 2022 02:02 PM	testprod@qualyssscmsdev.com	MEDIUM
UserLoggedIn	Office365 P26	Jan 6, 2022 02:01 PM	testprod@qualyssscmsdev.com	MEDIUM
Remove member from role	Office365 P26	Jan 6, 2022 01:37 PM	mjosshi@QualysSSCMSDev.com	LOW
Remove owner from group	Office365 P26	Jan 6, 2022 01:32 PM	Microsoft Teams Services	LOW

We have assigned a few categories and some specific sub-categories against each category to enable a better search and to ease the filtration.

For example, if you pick Authentication from Category options, User/Group and Application appear in the Sub-Category column.

The screenshot shows the 'Monitor' section of the SaaS Detection and Response interface with a search filter 'category: "Authentication"' applied. The table displays 2457 events. The left sidebar shows filters for SERVICE TYPE, CATEGORY, and SUB CATEGORY.

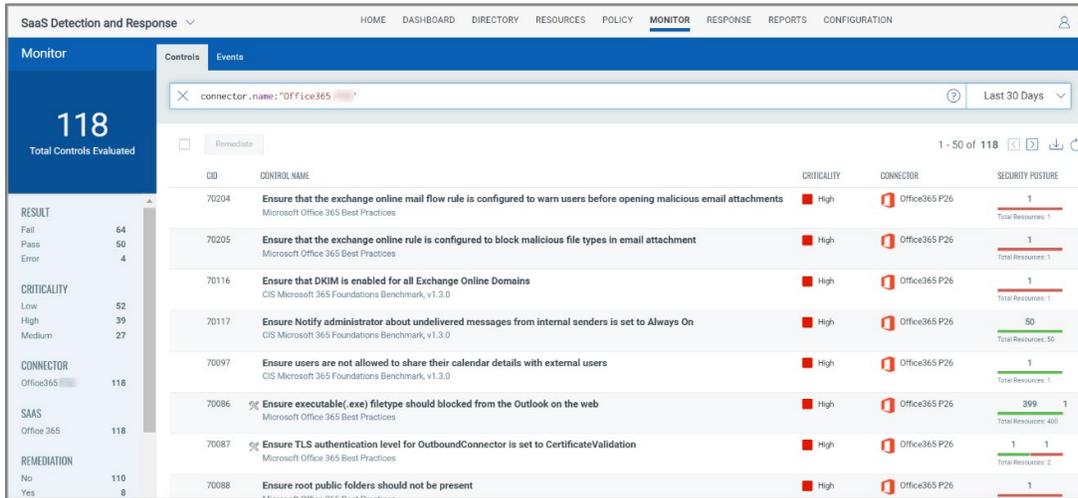
NAME	CONNECTOR	TIME	ACTOR	SEVERITY
UserLoggedIn	0365 QA p01	Feb 8, 2022 03:34 PM	testprod@qualyssscmsdev.com	MEDIUM
UserLoggedIn	0365 QA p01	Feb 8, 2022 03:32 PM	testprod@qualyssscmsdev.com	MEDIUM
UserLoggedIn	0365 QA p01	Feb 8, 2022 03:23 PM	testprod@qualyssscmsdev.com	MEDIUM
UserLoggedIn	0365 QA p01	Feb 8, 2022 03:21 PM	testprod@qualyssscmsdev.com	MEDIUM
UserLoggedIn	0365 QA p01	Feb 8, 2022 03:18 PM	testprod@qualyssscmsdev.com	MEDIUM
UserLoggedIn	0365 QA p01	Feb 8, 2022 03:18 PM	testprod@qualyssscmsdev.com	MEDIUM

The categorization parameters are set individually for each connector type based on the requirements and specifications of the apps.

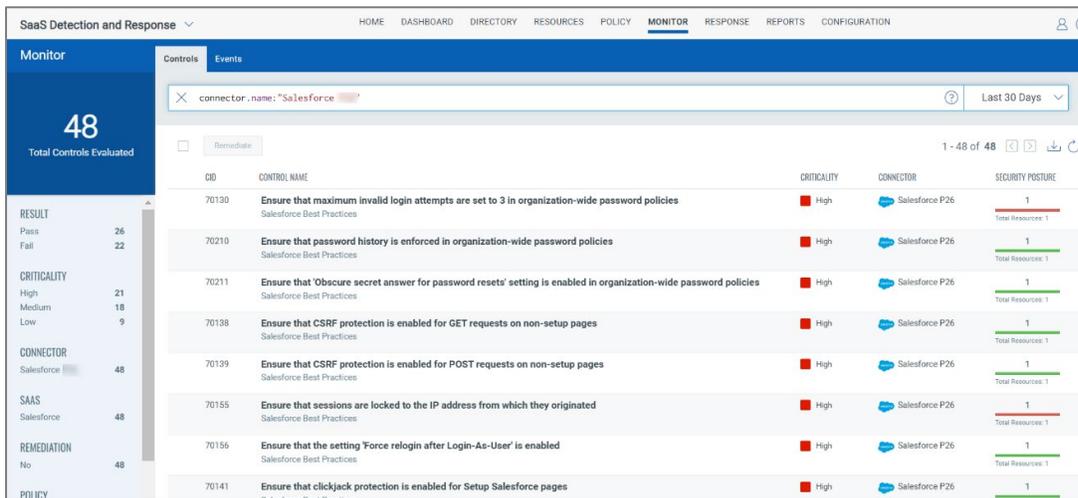
Content Updates

Following are some updates for this release:

Office 365 Controls - New controls are added to assess the compliance against the lateral attacks originating from ADFS setups. These controls help assess your organizational preparedness for preventing lateral movement of Solar Winds Attacks originating from the ADFS setup. To view the list of the controls, go to the **Monitor > Controls** tab. To refine your search, select the required connector from the **Connector** filter.



Salesforce Controls – SaaS DR is now publishing out-of-the-box controls as suggested in Salesforce Security Guide 2021 edition. New controls are added to the Control Library based on the Salesforce Security Guide 2021 edition. However, you can view the evaluations under the **Monitor > Controls** tab.



Salesforce Events - SaaS DR monitors all the events generated by Salesforce. All the events, including configuration changes, privilege escalations, failed logins, data exposure, apps with high exposure, and so on, are monitored in SaaS DR and listed under the **Monitor > Events** tab.