SaaS Detection and Response

Getting Started Guide
Version - 1.1.0

February 19, 2021
# Table of Contents

**About this Guide** ............................................................................................................. 4
About Qualys .......................................................................................................................... 4
Qualys Support ........................................................................................................................ 4

**SaaS Detection and Response Overview** ................................................................. 5
How to get started ................................................................................................................. 5

**Create Connector** .......................................................................................................... 6

**View User Directory** ...................................................................................................... 7

**View your Resources** ...................................................................................................... 8

**Monitor your Compliance Posture** ................................................................................ 9

**Dynamic Dashboard** ....................................................................................................... 15

**Working with Trusted Domains and Applications** ....................................................... 16
About this Guide

Welcome to Qualys SaaS Detection and Response (SaaSDR)! We’ll help you get acquainted with the Qualys solution on how to help enterprises with security and compliance of their SaaS applications using the Qualys Cloud Security Platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.
SaaS Detection and Response Overview

Qualys SaaS Detection and Response (SaaSDR) expands the capabilities of the Qualys Cloud Platform to help enterprises with security and compliance of their SaaS applications. It will provide a single console for IT admins to connect to their critical SaaS applications, manage them centrally, secure data on these critical cloud apps, maintain compliance and manage costs. It is a tool for IT admins to effectively manage SaaS sprawl.

Benefits of SaaSDR
- Provide a single console for IT admins to centrally secure their data no matter where it is
- Get a consolidated view of external users who have access to internal documents and internal users that are sharing documents externally
- Get visibility into documents that are exposed and take steps to make them private
- Get visibility into apps that have given access to sensitive data and take steps to alert and block them
- Take remediation actions to control exposure, remove access to external users, and mark sensitive documents private
- Understand the compliance posture of your critical SaaS applications to ensure that you pass industry standard benchmarks. Currently we support the CIS Microsoft 365 Foundations Benchmark

How to get started
Follow these steps to get started with SaaS Detection and Response.
- Configure your connectors
- View all the Users and User Groups
- View all your resources, like files and folders, and third party applications
- Run the CIS policy and view the policy controls to monitor your compliance posture
Create Connector

Start by creating a connector to your SaaS application.

Supported connectors for this release:
- Google G Suite
- Microsoft Office 365
- Zoom
- Salesforce (SFDC)

Let’s get started!

Choose SaaS Detection and Response (SaaSDR) from the app picker. You’ll need the SaaS application credentials to create the connector.

The steps to create a connector depends on the SaaS application you want to create the connector for. Refer the Create Connectors section of the Online Help for information on configuring your connector.

Once your Connector is created it will show in the Configurations > Connectors list. Here you can check the status and other details of the connector.

You’re ready!

Once the application is connected, a scan is initiated to pull meta data from the application. This step may take some time to complete based on the number of resources to be cataloged in your application.
View User Directory

As your scan progresses, the Directory tab is populated with all the users and user groups in the company that have access to the SaaS applications.

Navigate to Directory > Users or Groups tab and view the list of all users and user details what kind of access the user has: internal or external, role of the user, etc.
View your Resources

A list of resources such as files, folders, third party applications and meeting details are displayed in the Resources tab. You can view details such as what kind of access the resource has, who all the resources are shared with, owner, etc.

The Files and Folders tab lists the documents and folders in your company.

The Applications tab lists all the third-party applications that are installed by users in your company. You can view details like who has installed these applications using the company account and what permissions are granted. toggle between the Apps view to view this data grouped by the app name, and the Users view to view the count of apps installed by each user.

The Meetings tab lists all the meetings and webinars conducted via applications like Zoom. Note that the tab lists only those meetings that have at least one recording. Meetings that do not have recordings are not captured by SaaSDR.

Note: Qualys SaaSDR does not list on-going meetings or meetings scheduled for the future.

For SaaSDR to list a meeting, the meeting should be concluded and should have at least one cloud recording.
Monitor your Compliance Posture

You can run policies and benchmarks defined for your SaaS application. The controls are validated and the pass or fail status is displayed. For this beta version, we support MS O365 CIS Benchmarks.

Simply go to Policies tab to view all the policies provided by Qualys. From here you can also enable or disable the policy.

Navigate to the Monitor tab to monitor your compliance posture in real time. Here you can view the details of each control and the pass or fail status of that control.
Monitor your Compliance Posture

Enable Policy for Connector

You can run policies and benchmarks defined for your SaaS application. The controls are validated and the pass or fail status is displayed. Currently, MS O365 CIS Benchmarks is supported.

Simply go to the Policies tab to view all the policies provided by Qualys. From here, you can also enable or disable the policy for a connector.

Click on the policy to open it in the View Mode and navigate to the Connectors tab. Select a connector and from the Actions menu, enable or disable the policy for this connector.

The Controls tab lists all controls and their details such as connector type, criticality, etc. Click on any control to view details specific to that control.
Once a policy is enabled for a connector, you can view your compliance posture in the Monitor tab.

Note: For the following controls to be evaluated in SaaS DR accurately, make sure the "Apps that don't use modern authentication" setting is enabled in Microsoft 365 Admin Center > SharePoint > Policies > Access Control:  9036, 9037, 9038, 9018, 9012, 9007

Note: You must have a Microsoft 365 E5 license to evaluate the following 4 controls: 9010, 9011, 9025, 9026

Monitor Compliance Posture

In the Monitor tab, you can monitor your compliance posture in real time for each connector. View details such as connector type and the security posture at a quick glance.
Monitor your Compliance Posture

From the Security Posture column, you can drill down to view details of each control and their pass or fail status. Click on each control to view further details of the control such as remediation, evidence, etc.

Control References

Control references are available for different connectors in the application.
User can view references using specific controls as mentioned in the following sections.

**Controls in SFDC**

Control ID: 30027

For C Id: 30027, in evidence details, the password complexity is displayed in numbers.

Under Evidence column, user can click Show Details to view the evidence of control.

Click on ‘i’ icon to know more about the password complexity.

The meaning of number with respect to actual password complexity in salesforce is represented as follows:

0 - No restriction
1 - Must include alpha and numeric characters
2 - Must include alpha, numeric and special characters
3 - Must include numbers and uppercase and lowercase letters
4 - Must include numbers, uppercase and lowercase letters, and special characters
5 - Must include 3 of the following: numbers, uppercase and lowercase letters, and special characters
Monitor your Compliance Posture
Dynamic Dashboard

The Qualys SaaS DR application provides out-of-the-box default dashboard providing a summary of resources and compliance posture across resources.

A scan is initiated once the connector is successfully created and the scan results are displayed in various widgets of the dashboard.

Here you can view information such as the exposure of documents in the company, who all the documents are shared with internally and externally, what are the most shared documents and with which user, etc.

The default dashboard provides:
- Document Exposure
- Applications at risk
- All documents by type
- External users with most access
- Internal users with most exposure

Check out this sample dashboard:
Working with Trusted Domains and Applications

At times, when you work closely with members of a different domain, you might want to add resources of that domain as trusted resources. For example, when working with company XYZ on a project, you might end up sharing resources with members of this company. Qualys SaaS DR allows you to add domains and applications you trust to a trusted list. Once included in the list, you can use the Non Trusted or Is Trusted filters in the Resources > Applications tab to view resources from other domains.

Adding Domains and Applications as Trusted

Follow these steps to add domains and applications to the trusted list:

1. Navigate to the Configuration > Trusts tab and click New.

2. On the Create Trust screen, choose Domain or Application and define the value. Finally, click Create.
The created trust is listed in the Trusts tab.

Removing Domains and Applications from Trusted list

Follow these steps to remove a previously added domain/application from the Trust list:

1. Navigate to the Configuration > Trusts tab.
2. Select the applications/domains you wish to remove from the list and then click Actions > Delete to remove them from the list.