



Qualys SaaS Detection and Response (SaaS DR)

Release Notes

Version 1.7.0

September 01, 2022

Here's what's new in SaaS Detection and Response 1.7.0!

[CIS MS Office 365 Foundations Benchmark v1.4.0](#)

[Azure AD Content Enhancements](#)

[Assessment of MS 365 according to Conditional Access Policies](#)

[Updates in Non-CIS MS Office 365 Controls](#)

[Validation of Permissions and Roles for MS 365 Remediation](#)

[Connector Getting Stuck in Pending State Issue](#)

[Refresh Button on View Remediation Details Page](#)

CIS MS Office 365 Foundations Benchmark v1.4.0

We are now proud and only certified vendor of the latest version of CIS MS Office 365 benchmark. This benchmark provides a guidance for ensuring a secure configuration posture for Microsoft 365 SaaS offering. This benchmark contains recommendations for Exchange Online, SharePoint Online, OneDrive for Business, Teams, Azure Active Directory, and InTune.

With the new MS Office 365 Foundations Benchmark v1.4.0 release, SaaS DR updated the following controls:

CID	Statement	Operation	Reason
70098	Ensure users are not allowed to click through to the original URL in supported Office apps.	Removed	Deprecated by CIS
70184	Ensure that the Safe links scanning is enabled in supported Office 365 apps.	Removed	Deprecated by CIS
70119	Ensure that LinkedIn contact synchronization is disabled	Removed	Deprecated by Microsoft
70249	Ensure that the Safe links policy is enabled for Microsoft Teams	Added	

Azure AD Content Enhancements

Azure AD is a crucial component of MS 365 offering, which governs the access control to various services on MS 365 tenant. With this release, we are adding more checks to assess the hardening of Azure AD. Following controls are added with this release:

CID	Statement
70250	Ensure that the guest user has limited access
70252	Ensure that only administrators are allowed to invite the guest users
70253	Ensure that non-compliant devices are not present in the Azure AD tenant
70254	Ensure that stale devices are not present in the Azure AD tenant
70255	Ensure that rooted or jail-broken devices are not present in the Azure AD tenant
70256	Enable Conditional Access policy to enforce multi-factor authentication for guest and external users
70257	Enable Conditional Access policy to enforce multi-factor authentication for administrative roles
70258	Enable Conditional Access policy to enforce multi-factor authentication for devices using Azure AD join or register
70259	Enable Azure AD Identity Protection sign-in risk policies
70260	Enable Azure AD Identity Protection user risk policies

Assessment of MS Office 365 according to Conditional Access Policies

MS Office 365 allows the administrators to define the Conditional Access policies. Multiple Conditional Access policies can coexist for different users, and for different settings. Through these policies, administrators govern the configurations and access for individual users or a set of users.

When SaaS DR displays the controls on the **Monitor** page along with the posture, evidence details show how the control is getting evaluated for different conditional policies.

You can now search the control posture based on the name of a given conditional policy. This will enable you to view posture with respect to the policy or create specific widgets with respect to the policy.

RESOURCE	EVALUATED ON	RESULT	EVIDENCE
ConditionalAccessPolicy_1	Jun 21, 2022 03:00 PM	PASS	Show Details
ConditionalAccessPolicy_2	Jun 21, 2022 03:00 PM	PASS	Show Details
ConditionalAccessPolicy_3	Jun 21, 2022 03:00 PM	PASS	Show Details
ConditionalAccessPolicy_4	Jun 21, 2022 03:00 PM	FAIL	Show Details
ConditionalAccessPolicy_5	Jun 21, 2022 03:00 PM	FAIL	Show Details

Updates in Non-CIS MS Office 365 Controls

We evaluated some controls for the default policies and found that they had minimal to no security impact hence removed the following controls for the Non-CIS policy: 70000, 70001, 70005, 70006, 70009, 70010, 70014, 70025, 70027, 70028, 70030, 70031, 70032, 70037, 70049, 70052, 70054.

Validation of Permissions and Roles for MS Office 365 Remediation

In this new feature, SaaS DR facilitates the validation of appropriate permissions/roles assigned to the user or application before a Remediation Job can be submitted. The validations happen when the user clicks on the **Enable** button for a Remediation Job.

Connector Getting Stuck in Pending State Issue

The issue where the connector was getting stuck in the Pending (Scanning in progress) state is resolved now.

Refresh Button on View Remediation Details Page

A new Refresh button is added on the **View Remediation Details** page. It will refresh the remediation job status and the control remediation status.

The screenshot shows the 'View Details: 70016' page. On the left is a 'VIEW MODE' sidebar with 'Summary' selected. The main content area is titled 'Summary' and includes a refresh button in the top right corner. Below the title is a card for job 70016, created by 'dadasaheb.gopinath@gmail.com'. The 'Remediation Job Details' section shows 'Office 365' as the SaaS, 'o365 test' as the connector, and 'Completed' as the status. The 'Controls' section contains a table with one entry.

CID	NAME	REMEDIATION ACTION	CRITICALITY ↓	REMEDIATION STATUS
70016	Ensure users do not use Citrix ShareFile as...	Set-CsTeamsClientConfigurati...	High	Completed