

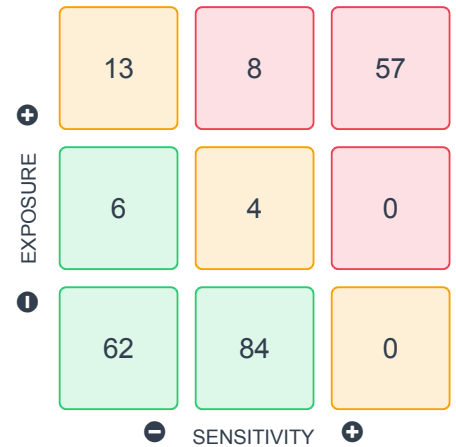
Risk Summary


What does risk mean for your organization?

The Overall Risk analyzes your organization external risk by looking at external guests or content shared outside against potential sensitive or confidential information as set by your Administrator according to rules for Microsoft 365 usage.

This helps to prioritize your risk to focus on what is important to your business.

Overall Risk






SENSITIVE ITEMS

167


↓ 8 in last 7 days



EXTERNAL LINKS

76


↓ 2 in last 7 days



EXTERNAL USERS IN AAD

19


↓ 18 in last 7 days



HIGH RISK ITEMS

146

↓ 17 in last 7 days



MEDIUM RISK ITEMS

13

↓ 106 in last 7 days

Direct Access Sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	13
Everyone except External Users	55
External Users	103
Anonymous Links	36
Links for Specific External Users	21



External Users with Highest Risk



NAME	SENSITIVE ITEMS
Adele Vance	96
Alex Wilber	12
Lidia Holloway	7







↓ ↑ Denotes change over the last 7 days



Microsoft Teams

 SENSITIVE ITEMS
44  1

 EXTERNAL LINKS
16  4

 EXTERNAL USERS WITH ACCESS
19  5

 HIGH RISK ITEMS
44  1

 MEDIUM RISK ITEMS
0  19

Teams Risk Summary

TYPE	COUNT
Total Teams	Public 27 Private 21 48
Teams with Guest Users <i>Guest users may unintentionally have access to confidential data distributed by your users.</i>	8
Teams with Shadow Users <i>External users may unintentionally have access to confidential data distributed by your users.</i>	12
Teams with High Risk Items <i>High risk Teams contain both sensitive information and out of policy exposure levels per defined policies.</i>	5
Teams without Available Owners <i>Teams without available owners may allow any user to have unchecked access to view or distribute sensitive data.</i>	6

Direct Access Sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	5
Everyone except External Users	22
External Users	32
Anonymous Links	7
Links for Specific External Users	8

Teams with Highest Risk

NAME	HIGH RISK ITEMS
Business Group	17
HR	17
Legal	5

High Risk Teams contain sensitive information and have exposure levels that are out of your defined policies.



↓ ↑ Denotes change over the last 7 days

SharePoint Online

SENSITIVE ITEMS

42

↓ 5

EXTERNAL LINKS

9

= 0

EXTERNAL USERS WITH ACCESS

12

= 0

HIGH RISK ITEMS

29

↓ 13

MEDIUM RISK ITEMS

6

↑ 6

SharePoint Online Risk Summary

TYPE	COUNT
Total Site Collections	41
Site Collections Shared with External Users <i>External users may unintentionally have access to confidential data distributed by your users.</i>	4
Site Collections with High Risk Items <i>High risk site collections contain both sensitive information and out of policy exposure levels per defined policies.</i>	2

Unique Permissions

TYPE	COUNT
Site	3
Library/List	7
Folder	9

Direct Access Sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	2
Everyone except External Users	13
External Users	14
Anonymous Links	5
Links for Specific External Users	2


Site Collections with Highest Risk

NAME	HIGH RISK ITEMS
Portal Manager Site	17
Security Information	12
Statistical Accounts	0




↓ ↑ Denotes change over the last 7 days

OneDrive for Business

 SENSITIVE ITEMS


47

↑ 11

 EXTERNAL LINKS


38

↑ 2

 EXTERNAL USERS WITH ACCESS


12

↓ 1

 HIGH RISK ITEMS

39

↓ 3

 MEDIUM RISK ITEMS

7

= 0

OneDrive Risk Summary

TYPE	COUNT
Total OneDrives	20
Shared via Anonymous Link	5
<i>Anonymous links can be viewed by anyone which may expose the organization security information widely.</i>	
Shared with External Users	4
<i>External users may unintentionally have access to confidential data distributed by your users.</i>	

High Exposure by Type

FOLDER TYPE	COUNT
Microsoft Teams Chat Files	2
Attachments	2

Direct Access Sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	6
Everyone except External Users	2
External Users	29
Anonymous Links	14
Links for Specific External Users	7

OneDrive with Highest Risk

NAME	HIGH RISK ITEMS
Jonas Coba	29
Laura Lash	10
John Paul	0

High risk OneDrives contain sensitive information and have exposure levels that are out of your defined policies.



↓ ↑ Denotes change over the last 7 days

Microsoft 365 Group

SENSITIVE ITEMS

34

↓ 2

EXTERNAL LINKS

13

= 0

EXTERNAL USERS WITH ACCESS

18

= 0

HIGH RISK ITEMS

34

↓ 3

MEDIUM RISK ITEMS

0

↓ 11

Microsoft 365 Groups Risk Summary

TYPE	COUNT
Total Microsoft 365 Groups	Public 23 Private 9 32
Microsoft 365 Groups with Guest Users <i>Guest users may unintentionally have access to confidential data distributed by your users.</i>	6
Microsoft 365 Groups with Shadow Users <i>Shadow users may have access to your Microsoft 365 Groups sensitive data through other areas of the Microsoft ecosystem without actually having permission in the Microsoft 365 site.</i>	6
Microsoft 365 Groups with High Risk Items <i>High risk Microsoft 365 Groups contain both sensitive information and out of policy exposure levels per defined policies.</i>	2
Microsoft 365 Groups without Available Owners <i>Microsoft 365 Groups without available owners may allow any user to have unchecked access to view or distribute sensitive data.</i>	3

Direct Access Sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	0
Everyone except External Users	18
External Users	28
Anonymous Links	10
Links for Specific External Users	4

Microsoft 365 Groups with Highest Risk

NAME	HIGH RISK ITEMS
DemoStreamGroup	17
Business Development	17
Statistical Accounts	0

High risk Microsoft 365 Groups contain both sensitive information and out of policy exposure levels per defined policies.



Exchange Online

We perform automated risk checks on Exchange Online settings and configurations. Any failed rules are flagged as potential security risks. However, an environment that passes all checks may not be entirely risk-free.



11

CHECKED RULES



8

PASSED RULES



3

FAILED RULES

Exchange Online

STATUS	RULES	RECOMMENDATIONS
Passed	Set Common Attachment Types filter <i>Set Common Attachment Types filter to allow users to block known and custom malicious file types from being attached to emails.</i>	
Passed	Set Exchange Online Anti-Spam policies <i>Set Exchange Online Anti-Spam policies to protect your organization's email from spam, including what actions to take if spam is detected.</i>	
Passed	Set automatic forwarding <i>Disable automatic forwarding to prevent users from auto-forwarding emails.</i>	
Passed	Set mail flow rules to not whitelist any domains <i>Set Exchange Online mail flow rules to ensure they do not whitelist any domains.</i>	
Failed	Set Client Rules Forwarding block <i>Enable Client Rules Forwarding block to prevent using client-side rules to forward emails to external recipients.</i>	Enable Client Rules Forwarding block.
Failed	Set Safe Links policy <i>Enable the Safe Links policy to allow emails that include URLs to be processed and rewritten if necessary.</i>	Enable the Safe Links policy.
Passed	Set Safe Attachments policy <i>Enable the Safe Attachments policy to extend malware protection. This includes routing all messages and attachments without a known malware signature to a special hypervisor environment. In that environment, a behavior analysis is performed using a variety of machine learning techniques to detect malicious intent.</i>	
Failed	Set Anti-Phishing policy <i>A default anti-phishing policy provides protection for all users. Set up custom anti-phishing policies to enable advanced protection features.</i>	Create anti-phishing policies.
Passed	Set DKIM policy for Exchange Online domains <i>Use DKIM to help prevent spoofer from sending data that looks like it is coming from your domain.</i>	

Passed Set Calendar Anonymous Sharing

Control whether users are allowed to share their calendars with anonymous users outside the organization.

Passed Set Mailbox Auditing for All Users

Control whether to enable mailbox audit logging for users.