AvePoint®

Data Security Risk Assessment

Prepared for Contoso Corporation

TABLE OF CONTENTS

> *"We need to be aware of the type of data we have, its sensitivity, and whether it contains patient or other personal data. AvePoint gives us this information, helping us stay in control of our data and keep up with growing cybersecurity concerns and the changing data privacy landscape."*

Tim van Toledo

Project Manager, ICMT, Franciscus Gasthuis & Vlietland

EXECUTIVE SUMMARY

This Data Security Risk Assessment was conducted on behalf of Contoso Corporation using the AvePoint Confidence Platform to identify and address security and exposure risks in Microsoft 365 and Google Workspace. It includes a thorough review of permissions and content sensitivity across multiple services and content on each platform.

Securing unstructured data is essential for meeting compliance obligations and preventing unauthorized exposure. Proactively addressing these findings lowers the risk of costly breaches and protects an organization's reputation. It also fosters trust with stakeholders and ensures that security measures align with business goals. This approach leads to stronger data governance, more resilient information management, and a safer environment overall.

The assessment identified several high-risk areas within Contoso Corporation's Microsoft 365 and Google Workspace environments, highlighting overexposed sensitive data, unnecessary external user access, and misconfigured sharing settings that could lead to data breaches. This report provides a detailed analysis of the risks detected, their potential impact, and recommended remediation steps to improve Contoso's overall data security posture.

CRITICAL FINDINGS

The AvePoint Confidence Platform performed a comprehensive scan of Contoso Corporation's environment, and revealed critical issues such as overexposed sensitive data, oversharing, and:

Sensitive Data Exposure
Sensitive data that is highly exposed to many users.

Shadow Permissions
Untracked or undocumented permissions.

Group Access
Large groups with unrestricted data access.

External Users
Over-permissioned external collaborators.

This report outlines our findings and actionable next steps to address these risks effectively to help enable secure AI usage within your organization.

For Contoso Corporation we recommend a "Do Now, Do Next, Do Later" approach to remediating oversharing and potential data overexposure in your tenant as a way to make progress.

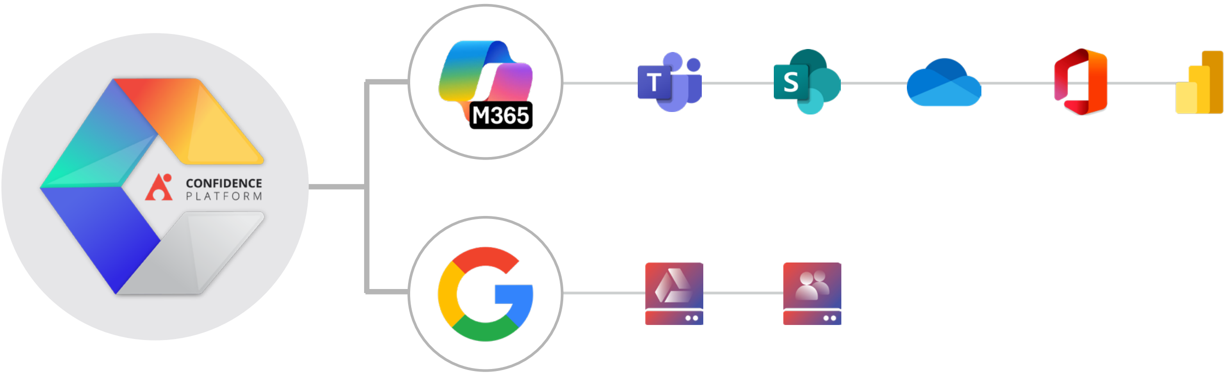
DO NOW	Implement these recommendations in the next two weeks.
DO NEXT	Implement these recommendations in the next four to five weeks.
DO LATER	Implement these recommendations in the next six to eight weeks (the sooner the better, of course).

OVERVIEW: OVERALL RISK & SENSITIVITY

Surface Area Scanned

AvePoint performed a comprehensive scan of Contoso Corporation's unstructured data and collaborative cloud content with the Confidence Platform, covering:

- **Microsoft 365:** Teams, SharePoint, OneDrive, Groups, Power BI
- **Google Workspace:** User Drives and Shared Drives
- **External Access & Sharing Links:** Analyzed permissions and sharing settings



This scan provided deep visibility into how sensitive data is stored, accessed, and shared within Contoso's cloud collaboration platforms. By examining data exposure, access controls, and permission settings, we identified vulnerabilities that could increase the risk of unauthorized access and potential data breaches. The findings and recommendations in this report aim to reduce these risks and ensure a more secure data environment.

The AvePoint Difference

01.

Proactive Data Governance

Ensure security from the start by enforcing policies that guide users to make the right decisions, every time.

02.

Automated Operational Governance

Eliminate security gaps with automated processes like lifecycle management and access reviews.

03.

Integrated Resilience

Go beyond traditional security by combining data security posture management with best-in-class backup and recovery.

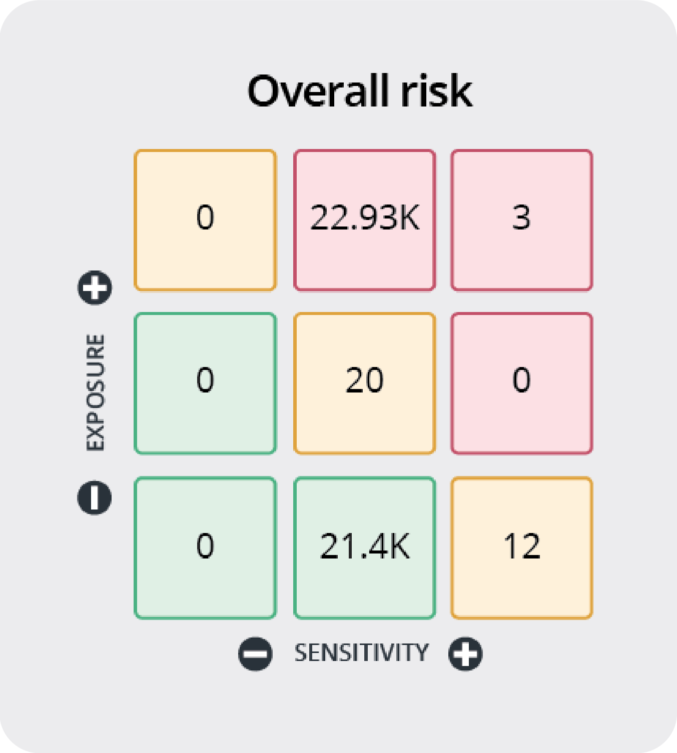
Risk Overview: Heatmap

All organizations have sensitive data, but this is not a problem until that data is overexposed to individuals that should not have access.

The risk assessment findings are visualized in a **heat map** with **EXPOSURE** on the vertical axis and **SENSITIVITY** on the horizontal axis.

Particular attention should be paid to the top-right quadrant, as this shows identified instances of high exposure and high sensitivity and should be remediated with high priority.

AvePoint's approach for Copilot and Gemini Data Readiness remediation is to help you identify where you have overexposed sensitive data as can be seen in the figure to the right.



Overall risk

0	22.93K	3
0	20	0
0	21.4K	12

DO NOW

AvePoint Recommends:

For Contoso Corporation, AvePoint uncovered 3 items flagged as highly-sensitive and highly-exposed, which are detailed in the next section. These items should be manually reviewed by Contoso Corporation's IT admin, together with the appropriate business owners, to resolve these as the highest priority. The detailed findings of these items are in the Detailed Findings section under 'High Sensitivity + High Exposure' section.

Risk Overview: By Platform

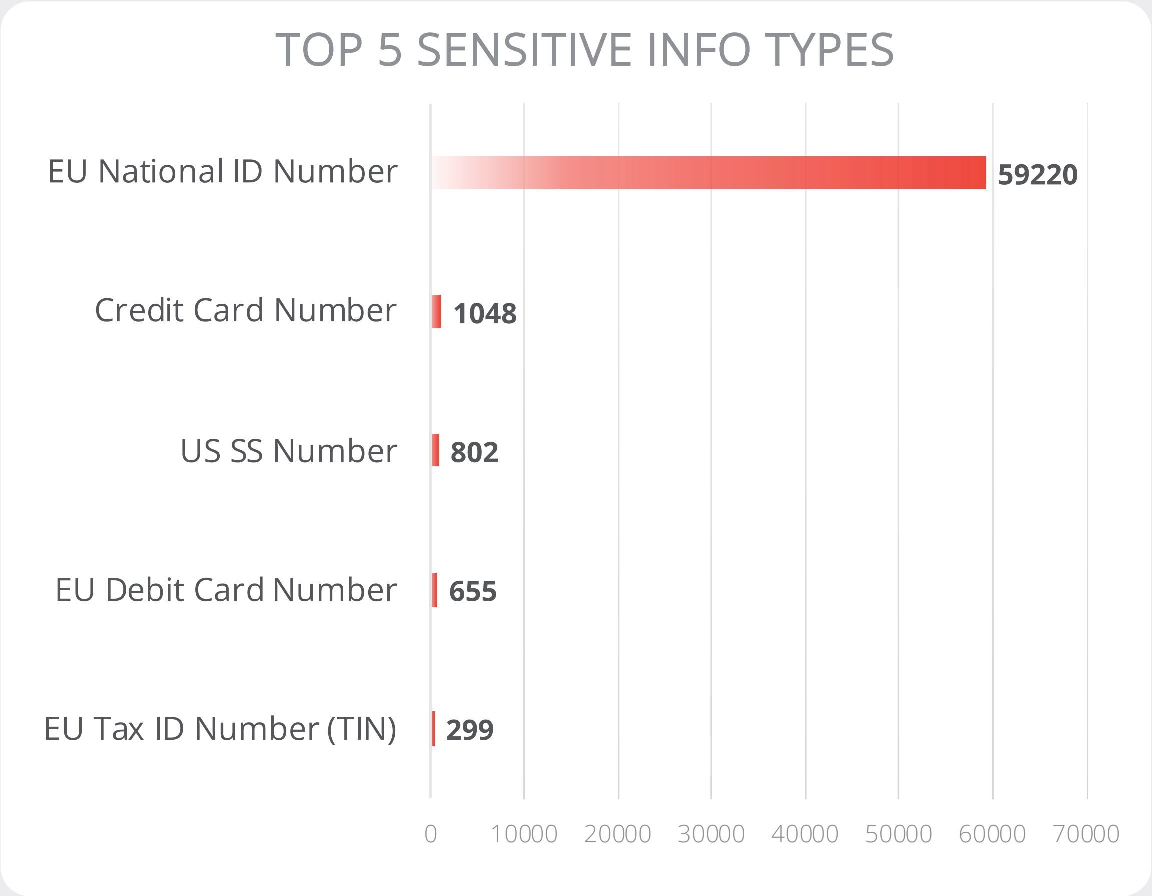
MICROSOFT 365

Microsoft Teams	744 TOTAL TEAMS	5 HIGH RISK TEAMS	35 TEAMS WITH GUEST USERS	52 TEAMS WITH HIGH RISK ITEMS
SharePoint Online	279 TOTAL SITE COLLECTIONS	6 HIGH RISK SITE COLLECTIONS	1 SITE COLLECTIONS SHARED WITH EXTERNAL USERS	23 SITE COLLECTIONS WITH HIGH RISK ITEMS
OneDrive	99 TOTAL ONEDRIVES	0 HIGH RISK ONEDRIVES	14 ONEDRIVES SHARED VIA LINK	13 ONEDRIVES SHARED WITH EXTERNAL USERS
M365 Groups	121 TOTAL M365 GROUPS	0 HIGH RISK M365 GROUPS	3 M365 GROUPS WITH GUEST USERS	6 M365 GROUPS SHARED WITH HIGH RISK ITEMS

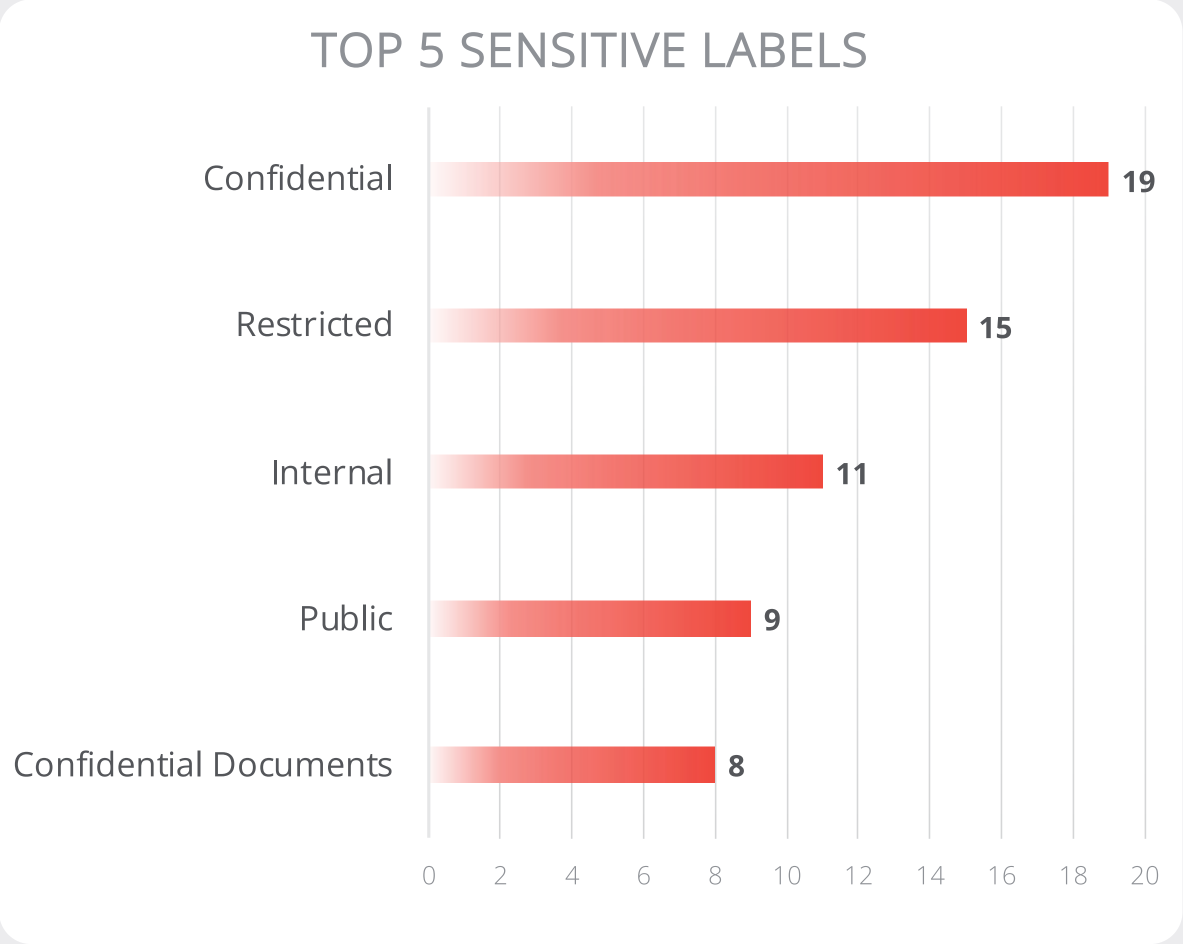
GOOGLE WORKSPACE

User Drive	3 TOTAL USER DRIVES	1 USER DRIVES SHARED WITH ANYONE VIA LINK	2 USER DRIVES SHARED WITH EXTERNAL USERS	1 USER DRIVES WITH HIGH RISK ITEMS
Shared Drive	1 TOTAL SHARED DRIVES	1 SHARED DRIVES SHARED WITH ANYONE VIA LINK	1 SHARED DRIVES WITH HIGH RISK ITEMS	0 HIGH RISK SHARED DRIVES

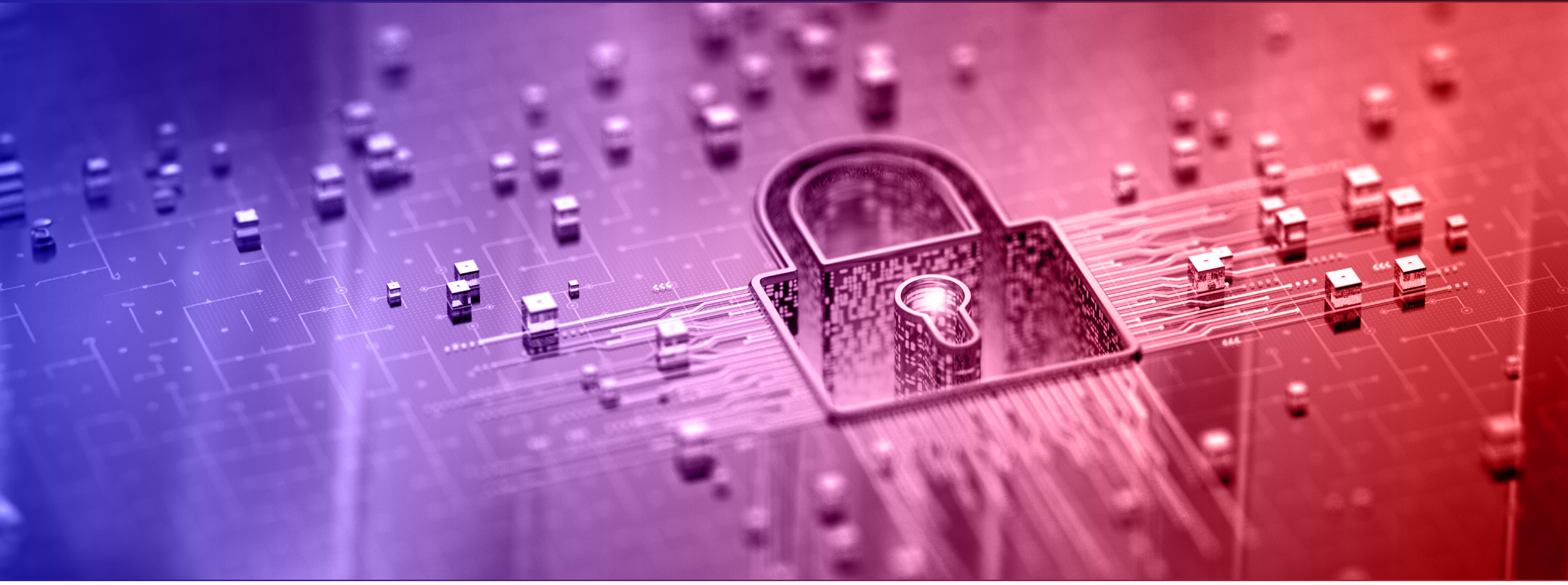
Risk Overview: Top Sensitive Items Discovered



This visualization highlights the predominant types of sensitive information found within Contoso Corporation's data environment. The substantial presence of EU National ID Numbers indicates a heightened risk of exposure, which requires proactive data protection measures to ensure they are protected. Credit Card Numbers and Social Security Numbers, though fewer in occurrence, still pose significant regulatory and security concerns. Identifying these trends enables Contoso Corporation to prioritize mitigation strategies, ensuring compliance with data governance standards while minimizing exposure to potential breaches.



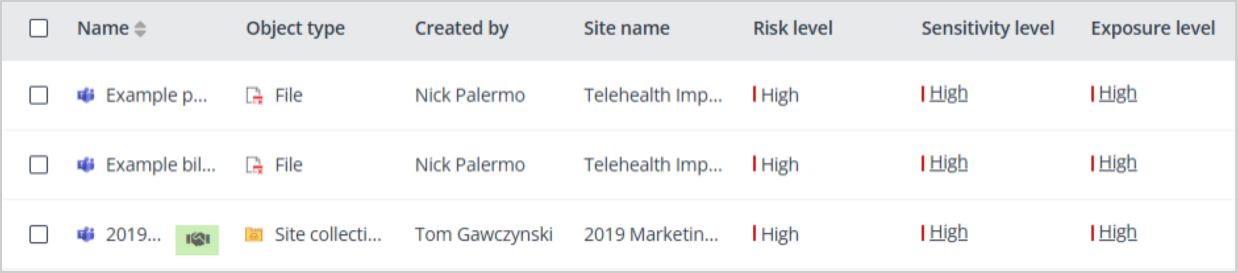
The prevalence of sensitive labels within Contoso Corporation's data landscape reflects an organizational effort to categorize and secure confidential information. The "Confidential" label leading the pack actually underscores a strong emphasis on safeguarding critical data assets. Similarly, the distribution of "Restricted" and "Internal" classifications highlights the need for strict access controls and policy enforcement. This is a great first-step, and continuing to strengthen the governance frameworks around these labels ensures sensitive data remains appropriately protected, reducing unauthorized access risks.



DETAILED RESULTS

High Sensitivity + High Exposure

The items in the table below should be reviewed with the highest priority. These files contain high-risk sensitive content (such as personal health information, billing information, Confidential tags, etc.) and are shared with 'Everyone' or equivalent.



□	Name	Object type	Created by	Site name	Risk level	Sensitivity level	Exposure level
□	Example p...	File	Nick Palermo	Telehealth Imp...	High	High	High
□	Example bil...	File	Nick Palermo	Telehealth Imp...	High	High	High
□	2019...	Site collecti...	Tom Gawczynski	2019 Marketin...	High	High	High

DO NOW

AvePoint Recommends:

Begin by reviewing the location of highly sensitive and highly exposed content to understand the business context. Consider reaching out to the workspace owner, both to notify of them of the sensitive information and to help raise awareness of correct data sharing policies.

DIRECT ACCESS SHARING (SENSITIVE CONTENT)

The assessment identified **27 direct access links** that are specifically related to items containing sensitive content.

5 "everyone except external" links
(widely accessible within the company)

3 anonymous links
(publicly accessible without authentication)

1 external/orphaned user link
(potential unauthorized retention of access)

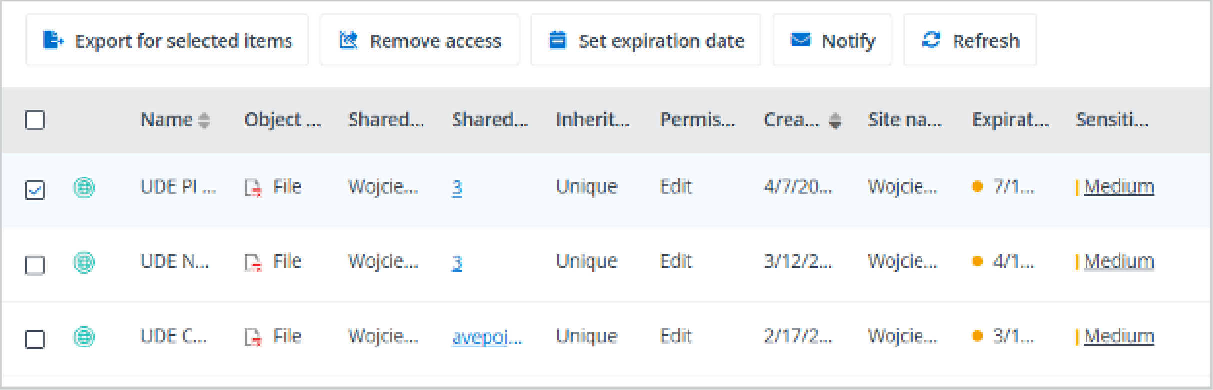
18 organizational links
(broad internal access)

Direct access sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	0
Everyone except external users	5
Anonymous link	3
Link for specific external/orphaned users	0
Organization link	18

These links increase the risk of unintentional data leaks, unauthorized access, and compliance violations. Sensitive data should be shared in a controlled manner, with explicit owner approvals and stricter permission settings.

The following Anonymous links discovered during the scan of Contoso Corporation should be acted upon immediately.



□		Name	Object ...	Shared...	Shared...	Inherit...	Permis...	Crea...	Site na...	Expirat...	Sensiti...
☑		UDE PI ...	File	Wojcie...	3	Unique	Edit	4/7/20...	Wojcie...	● 7/1...	Medium
□		UDE N...	File	Wojcie...	3	Unique	Edit	3/12/2...	Wojcie...	● 4/1...	Medium
□		UDE C...	File	Wojcie...	avepoi...	Unique	Edit	2/17/2...	Wojcie...	● 3/1...	Medium

Detailed descriptions of the sensitive items found, such as credit card or social security numbers, can be found within the online report by exploring the sensitivity.

DO NOW

AvePoint Recommends:

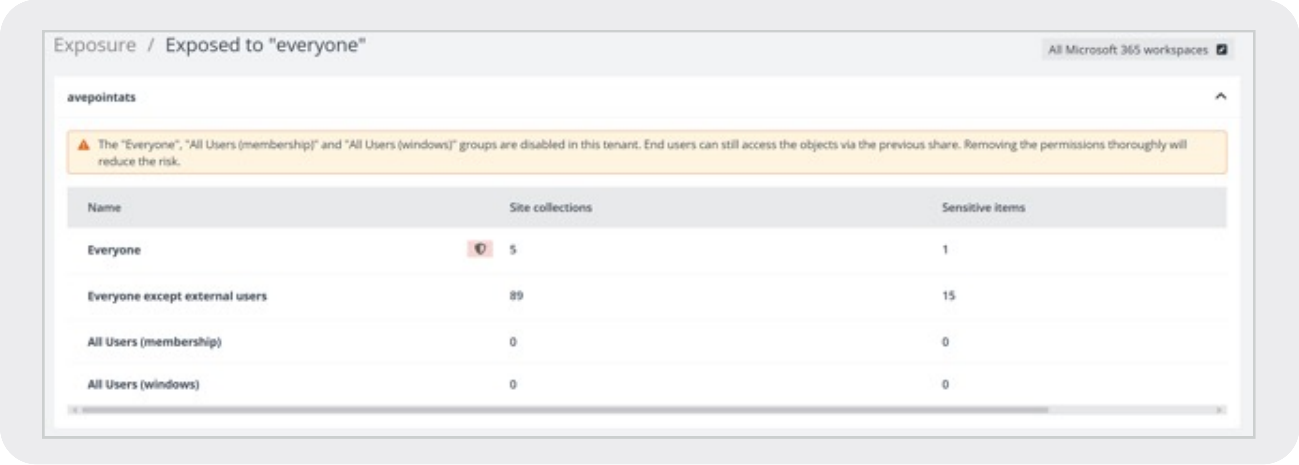
We recommend reviewing and removing the Anonymous links on Sensitive items immediately. While the items below are flagged as "Medium" risk based on their content, the fact they are shared via an Anonymous link should be addressed first.

We also recommended reviewing all items below, restricting "Everyone Except External" access where unnecessary, and consider implementing expiration and/or recertification policies to prevent accumulation.

LARGE GROUP ACCESS

When large groups have access to data, it increases the risk of overexposure by allowing more individuals than necessary to access sensitive information.

We've identified where you have instances of "Everyone" groups assigned access to documents within your tenant, including those with sensitive items.



Exposure / Exposed to "everyone"

All Microsoft 365 workspaces

avepointats

⚠ The "Everyone", "All Users (membership)" and "All Users (windows)" groups are disabled in this tenant. End users can still access the objects via the previous share. Removing the permissions thoroughly will reduce the risk.

Name	Site collections	Sensitive items
Everyone	5	1
Everyone except external users	89	15
All Users (membership)	0	0
All Users (windows)	0	0

DO NEXT

AvePoint Recommends:

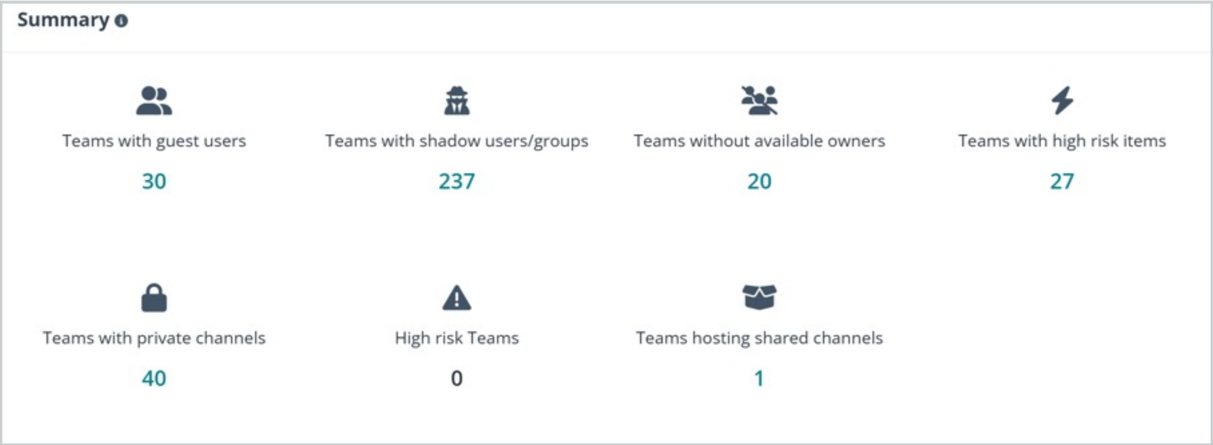
Reviewing sensitive items that have been exposed to large groups. You can also consider creating a policy that would prohibit large groups from being given access to resource in specific containers.

SHADOW PERMISSIONS

Microsoft Teams is essential for modern collaboration. It enables chat, file sharing, and integrated apps for teams spread across different locations. However, each team also has a SharePoint site that manages documents and permissions, which can unintentionally create “shadow users” if not managed carefully. These individuals might retain access after leaving the organization or moving into new roles, leaving sensitive data exposed.

One of the challenges with out-of-the-box reporting is that it only provides a partial view of who has access to what. This limited visibility makes it hard to spot and remove shadow users, especially when they have privileges across multiple Microsoft 365 services. It also opens the door to compliance issues if confidential information, like financial records or personal data, falls into the wrong hands.

The AvePoint Confidence Platform digs deeper than native tools and maps each user’s permissions across Teams and SharePoint. It flags hidden access and shows exactly which documents or folders are at risk. By classifying data and highlighting the most sensitive content first, security teams can deal with the highest-risk exposures right away. This approach reduces the time spent hunting for issues and ensures you can maintain secure collaboration without restricting the benefits of Microsoft Teams.



Summary

Teams with guest users
30

Teams with shadow users/groups
237

Teams without available owners
20

Teams with high risk items
27

Teams with private channels
40

High risk Teams
0

Teams hosting shared channels
1

DO NEXT

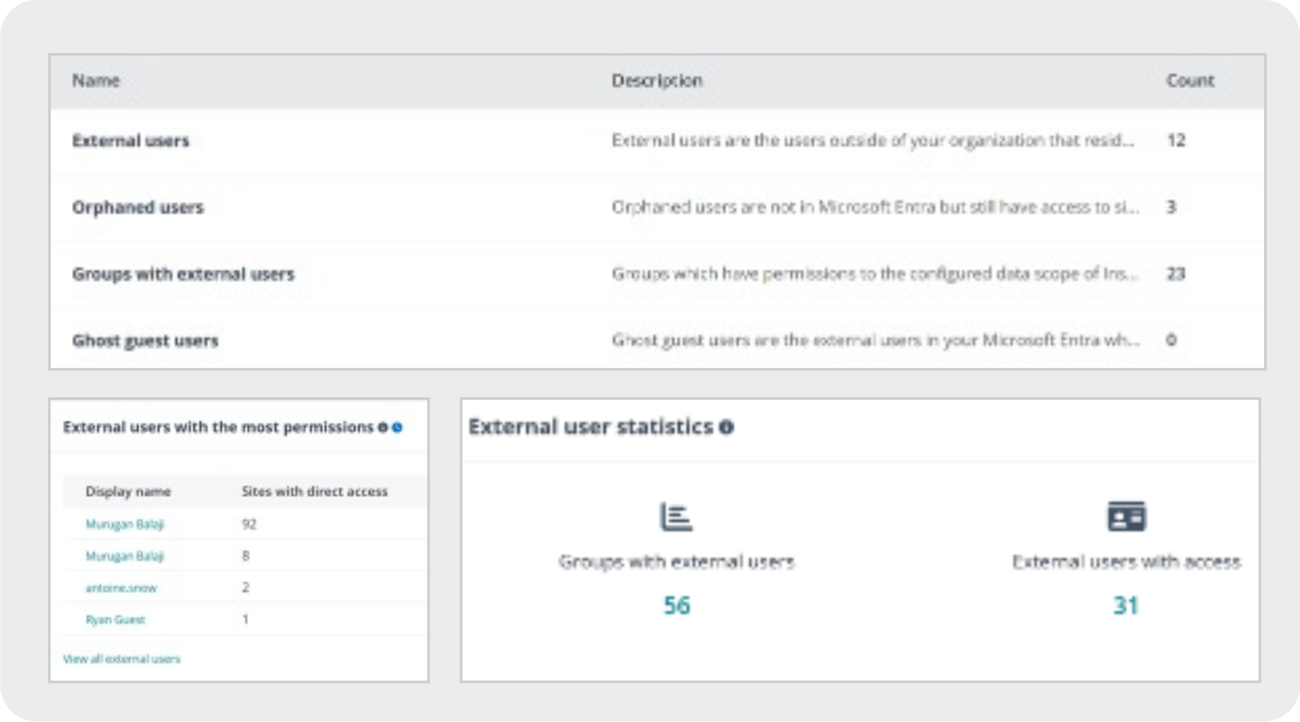
AvePoint Recommends:

Creating a rule that will remove Shadow Users & Groups from backend SharePoint sites to help reduce accidental overexposure of data. This policy can also provide an alert to users reminding them of the proper way to enable sharing.

EXTERNAL USERS

Effectively managing external user access is crucial for maintaining a secure and compliant Microsoft 365 environment. While these users often play key roles in collaboration, unchecked access can lead to unintended data exposure and potential security risks.

Properly governing permissions helps ensure that only necessary information is shared, reducing vulnerabilities and supporting overall data integrity within the organization.



Name	Description	Count
External users	External users are the users outside of your organization that resid...	12
Orphaned users	Orphaned users are not in Microsoft Entra but still have access to si...	3
Groups with external users	Groups which have permissions to the configured data scope of Ins...	23
Ghost guest users	Ghost guest users are the external users in your Microsoft Entra wh...	0

External users with the most permissions

Display name	Sites with direct access
Murugan Balaji	92
Murugan Balaji	8
antoine.snow	2
Ryan Guest	1

External user statistics

Groups with external users	External users with access
56	31

DO LATER

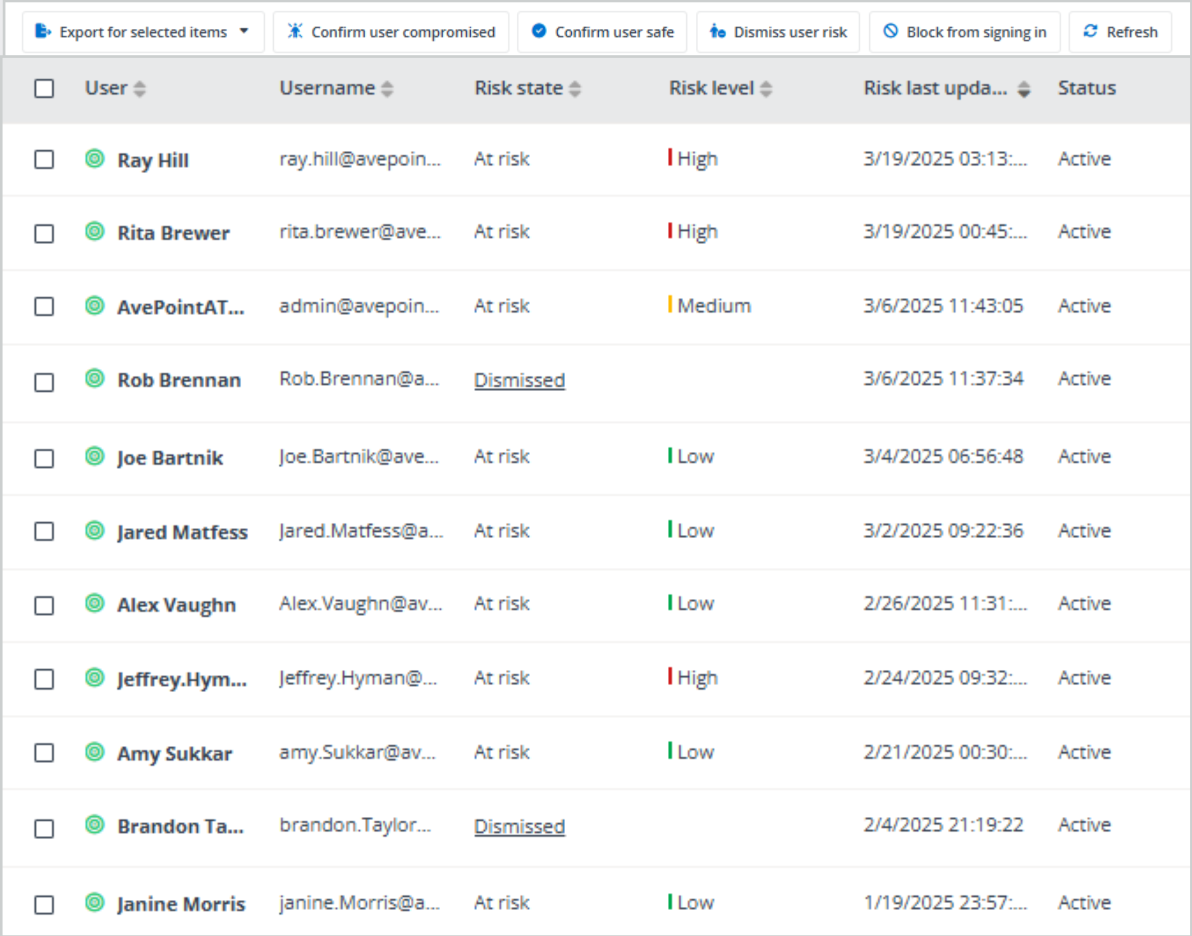
AvePoint Recommends:

Consider implementing a lifecycle management process to validate that external users still require access to your tenant. You can also consider setting an inactivity period that will remove access after a specified period of time.

RISKY USERS

The following users have been discovered with an activity history that could be deemed as suspicious based on existing patterns. Please note that being flagged on this page does not immediately indicate bad intent, rather a pattern of actions that may warrant closer inspection.

From this page, administrators can take additional actions such as reviewing further detailed actions, marking a user as 'confirmed safe' or 'confirmed compromised', blocking user from signing in, or more.



□	User	Username	Risk state	Risk level	Risk last upda...	Status
□	Ray Hill	ray.hill@avepoin...	At risk	High	3/19/2025 03:13:...	Active
□	Rita Brewer	rita.brewer@ave...	At risk	High	3/19/2025 00:45:...	Active
□	AvePointAT...	admin@avepoin...	At risk	Medium	3/6/2025 11:43:05	Active
□	Rob Brennan	Rob.Brennan@a...	Dismissed		3/6/2025 11:37:34	Active
□	Joe Bartnik	Joe.Bartnik@ave...	At risk	Low	3/4/2025 06:56:48	Active
□	Jared Matfess	Jared.Matfess@a...	At risk	Low	3/2/2025 09:22:36	Active
□	Alex Vaughn	Alex.Vaughn@av...	At risk	Low	2/26/2025 11:31:...	Active
□	Jeffrey.Hym...	Jeffrey.Hyman@...	At risk	High	2/24/2025 09:32:...	Active
□	Amy Sukkar	amy.Sukkar@av...	At risk	Low	2/21/2025 00:30:...	Active
□	Brandon Ta...	brandon.Taylor...	Dismissed		2/4/2025 21:19:22	Active
□	Janine Morris	janine.Morris@a...	At risk	Low	1/19/2025 23:57:...	Active

DO LATER

AvePoint Recommends:

Manually sort the list by Risk level with “High” as a top priority. Review the activities and details of each user carefully and take further action if appropriate.

Beyond Secure. **AvePoint Secure.**

Security isn't just about identifying risks – it's about taking action. Secure, govern, and protect your most sensitive cloud data with AvePoint's proactive approach to DSPM.

> *"AvePoint Confidence Platform provides much-needed governance and oversight capabilities for our digital landscape and cloud services. The vendor takes pride in listening to their customers' needs and working with them to enhance their product offerings. The tool-sets on offer are essential for complex environments."*
>
> **Group Product Manager, Public Sector**
> **Gartner Peer Insights, Data Security Posture Management Review 2025**

Setting the Standard for Secure Data Protection

Microsoft's Go-To Partner

Decades of collaboration with Microsoft, supporting customers globally with certified solutions

FedRAMP Authorized Solutions

Recognized by customers for our digital workplace solutions

Cloud Computing & SaaS

Recognized by customers for our digital workplace solutions

A Leader in Data Protection

4.6/5 rating for Multi-SaaS Backup-as-a-Service platforms

Best Enterprise-Level SaaS Product

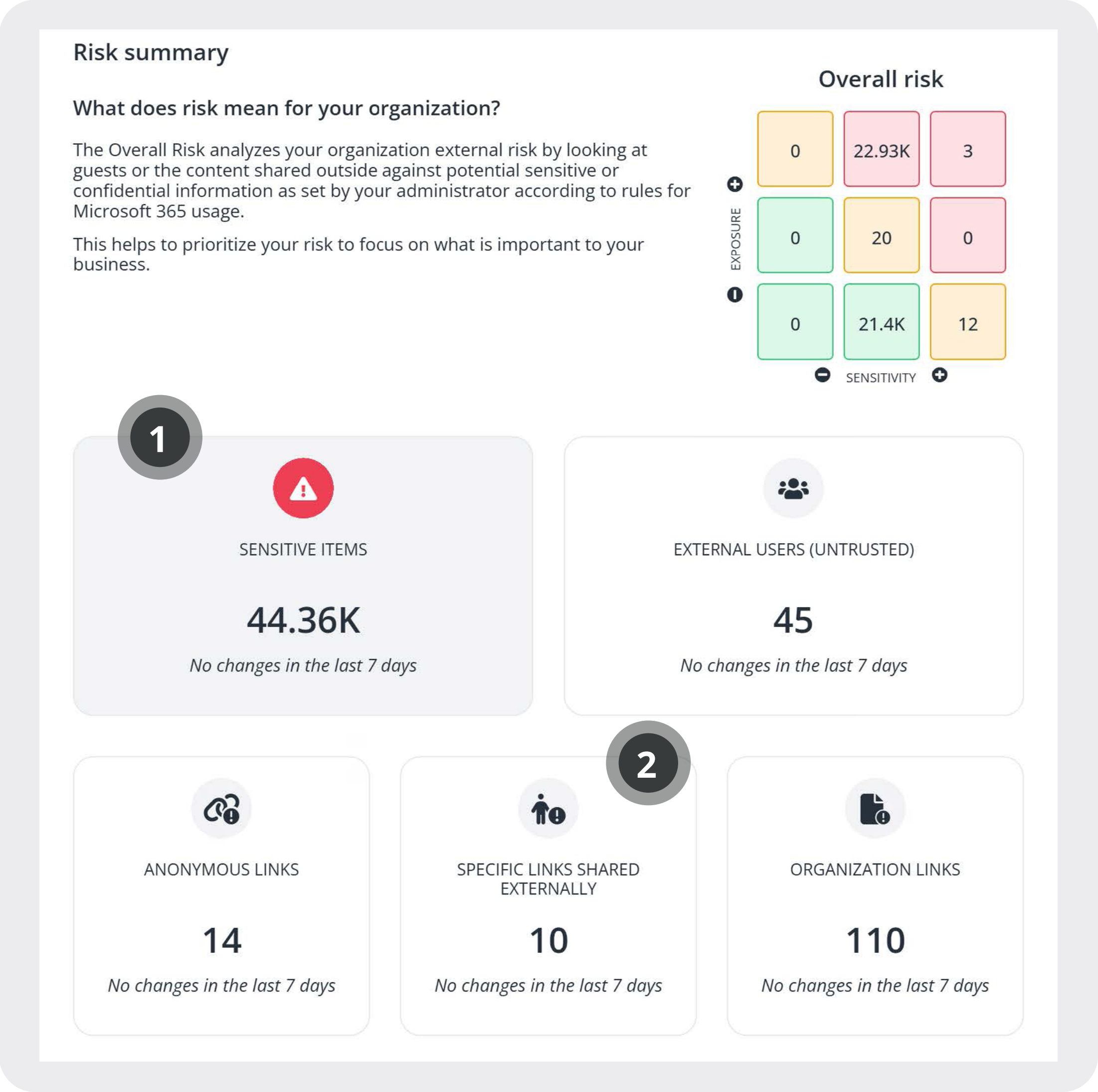
Recognized for innovation in SaaS operations and securing collaboration

SaaS Application Data Protection

Recognized as leader with highest current offering score

APPENDIX: SCAN REPORT EXPORT

In the following Appendix, the direct outputs of the scan export (used for making our detailed recommendations) have been included.



Risk summary

What does risk mean for your organization?

The Overall Risk analyzes your organization external risk by looking at guests or the 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

EXPOSURE ↑	SENSITIVITY –		SENSITIVITY +
+	0	22.93K	3
	0	20	0
–	0	21.4K	12

1

SENSITIVE ITEMS

44.36K

No changes in the last 7 days

EXTERNAL USERS (UNTRUSTED)

45

No changes in the last 7 days

ANONYMOUS LINKS

14

No changes in the last 7 days

2

SPECIFIC LINKS SHARED EXTERNALLY

10

No changes in the last 7 days

ORGANIZATION LINKS

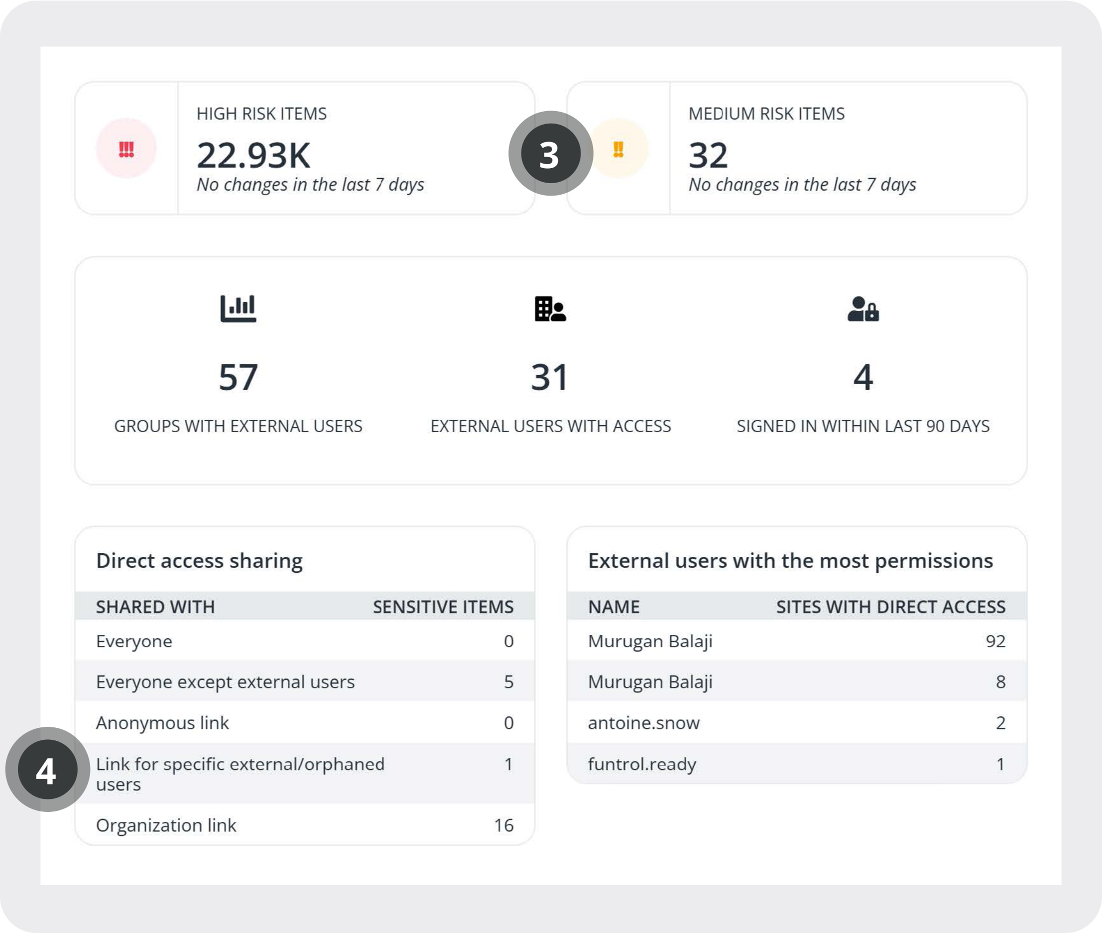
110

No changes in the last 7 days

1. The presence of sensitive items indicates that this site should be regulated more strictly than other team and collaboration workspaces. Sites containing high risk items should be audited and access should be recertified on a regular basis. If the site is not meant to host sensitive content, we recommend migrating that data to an appropriate site.

2. Data breaches often originate in the supply chain. Its always good to secure external access to your data. We recommend limiting access to specific files and folders, and avoid granting access to external users for entire sites.

**The data contained in this report is accurate as of your last scan.*



HIGH RISK ITEMS
22.93K
No changes in the last 7 days

MEDIUM RISK ITEMS
32
No changes in the last 7 days

57
GROUPS WITH EXTERNAL USERS

31
EXTERNAL USERS WITH ACCESS

4
SIGNED IN WITHIN LAST 90 DAYS

Direct access sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	0
Everyone except external users	5
Anonymous link	0
Link for specific external/orphaned users	1
Organization link	16

External users with the most permissions

NAME	SITES WITH DIRECT ACCESS
Murugan Balaji	92
Murugan Balaji	8
antoine.snow	2
funtrol.ready	1

3 Risk scores are calculated based on a combination of factors. Sensitivity of the data, location of the data, the number of users who have access, the types of users who have access (internal, external, admin, etc.), the type of access (read, write, download, etc.), based on pre-built or custom classifications and sensitivity labels.

4 While orphaned users may be unlicensed and have their access terminated it is possible for malicious actors to gain access to these accounts. During user offboarding there could have been an administrative error that does not lead to appropriate termination, there could be delays in processing, etc. Additional unauthorized users may gain access to this data through user impersonation or after account transfer to a replacement user or manager and reactivation. These new users may not be authorized to access this data. It is recommended to terminate this access quickly.

Stop Guessing. Start Securing.

AvePoint's award-winning Confidence Platform goes beyond traditional security, empowering your users to integrate secure practices right from the start. Take the first step towards implementing DSPM with a personalized Data Security Risk Scan.

See your security gaps before attackers do. Get your free personalized risk assessment today.

AvePoint
Data Security Risk Assessment
Prepared for Contoso Corporation
AvePoint

GET YOUR ASSESSMENT

What's included in your free risk scan?

At-Risk Data Report

Identify exposed sensitive files across Microsoft 365 including those with high exposure, missing classification, or files shared too broadly.

Workspace Governance Status Check

See which workspaces may pose a risk based on ownership, sensitivity, and activity history.

Data Quality Summary

Review the redundant, obsolete, and trivial (ROT) data living in your environment.

Actionable Fixes

Get clear, expert-backed recommendations to remediate issues and strengthen your data security.