Lepide

USE CASE GUIDE

HOW TO USE LEPIDE TO REPORT ON EXTERNAL DATA SHARING IN MICROSOFT 365

Table of Contents

1. Introduction

The external sharing capabilities in M365 make it easy for people within an organization to collaborate on projects with others outside who don't have an account in their directory.

They can collectively share, edit, and comment on documents making working together and sharing information streamlined and efficient.

The problem with this is that it is very easy for employees to accidentally share sensitive data. Often, the case is that employees are unaware that certain documents contain sensitive information and therefore should not be shared.

Over time, as users send unrestricted links to external contacts and download files to their devices, keeping track of where sensitive data has been sent becomes almost impossible.

2. Auditing within Microsoft 365

Microsoft 365 does offer some auditing, but it leaves a lot to be desired. There are event logs available, but no one has the time or inclination to examine thousands of M365 event logs and format them into a readable report. Doing this once would be a challenge, but on a regular basis would be an unrealistic expectation.

Another limitation of Microsoft 365 native auditing is that it only allows you to store the audit logs for 90 days. This means that constant manual review of the logs is necessary and investigations into historic incidents cannot take place.

3. The Solution

These limitations can be overcome by using the Lepide Data Security Platform. With this Solution, audit trails are stored for years, and the reports are easily searchable, sortable, and filterable so that you can retrieve all the information you need, whenever you need it, quickly and efficiently.

Lepide can show you when your data is being shared externally on M365, whether through public/private channels or individual chats. This gives you the ability to identify and alert in real time when your most sensitive data is being shared outside your organization, helping you to detect incidents that could lead to potential data breaches.

Running the 0365 External Data Sharing Report allows you to see immediately what has been shared, who has shared it and when it occurred. The report can then be filtered as required to allow you to focus on the specific areas you need to explore.

4. The External Data Sharing m365 Report

4.1. Prerequisites

Before running the report, you will need to have configured the Lepide Data Security Platform for Microsoft 365.

4.2. Running the Report

From the component management window, click on the Permission & Privileges  icon

Expand **Risk Analysis**

Click on **External Data Sharing M365**

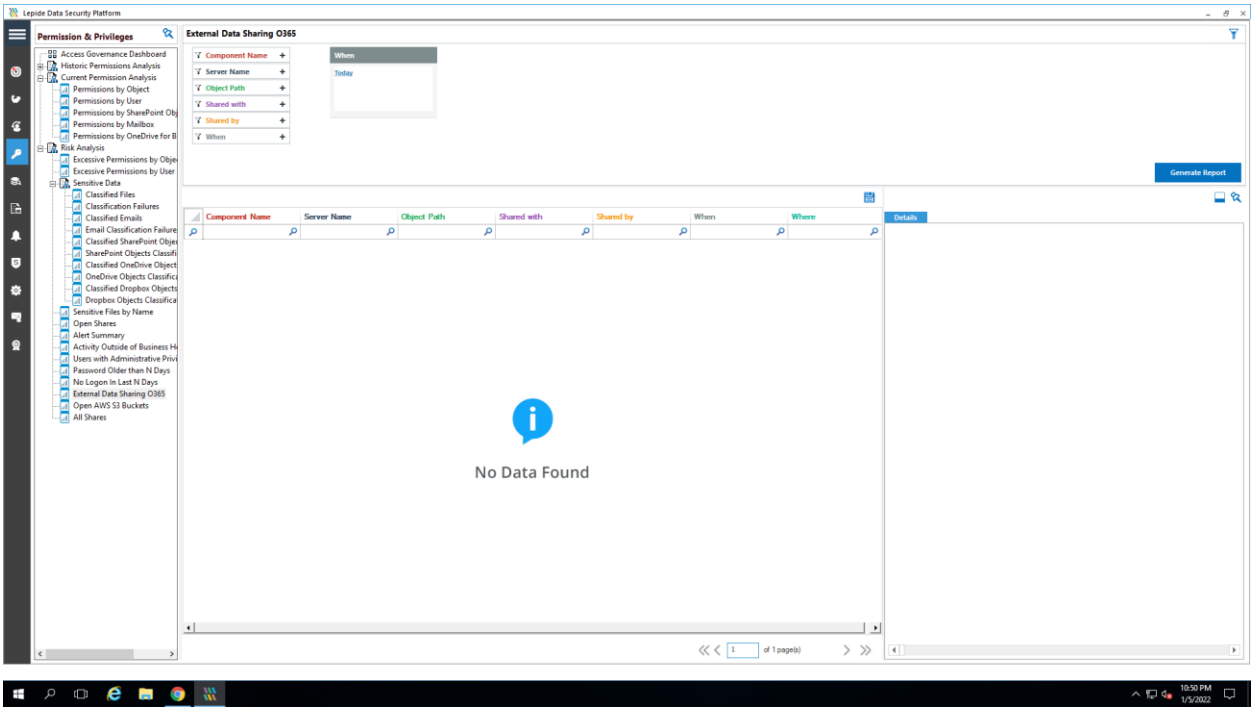

Figure 1: External Data Sharing M365

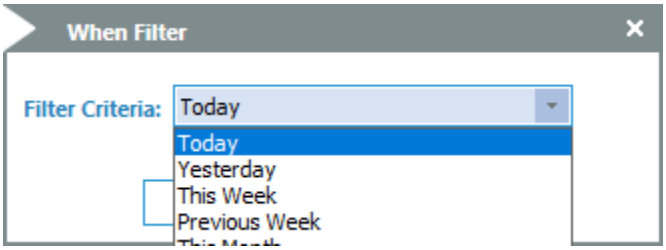

Figure 2: The 'When' Filter

From the **When** filter at the top of the screen, choose a date range for the report:

Click **OK**

Then click the **Generate Report** button

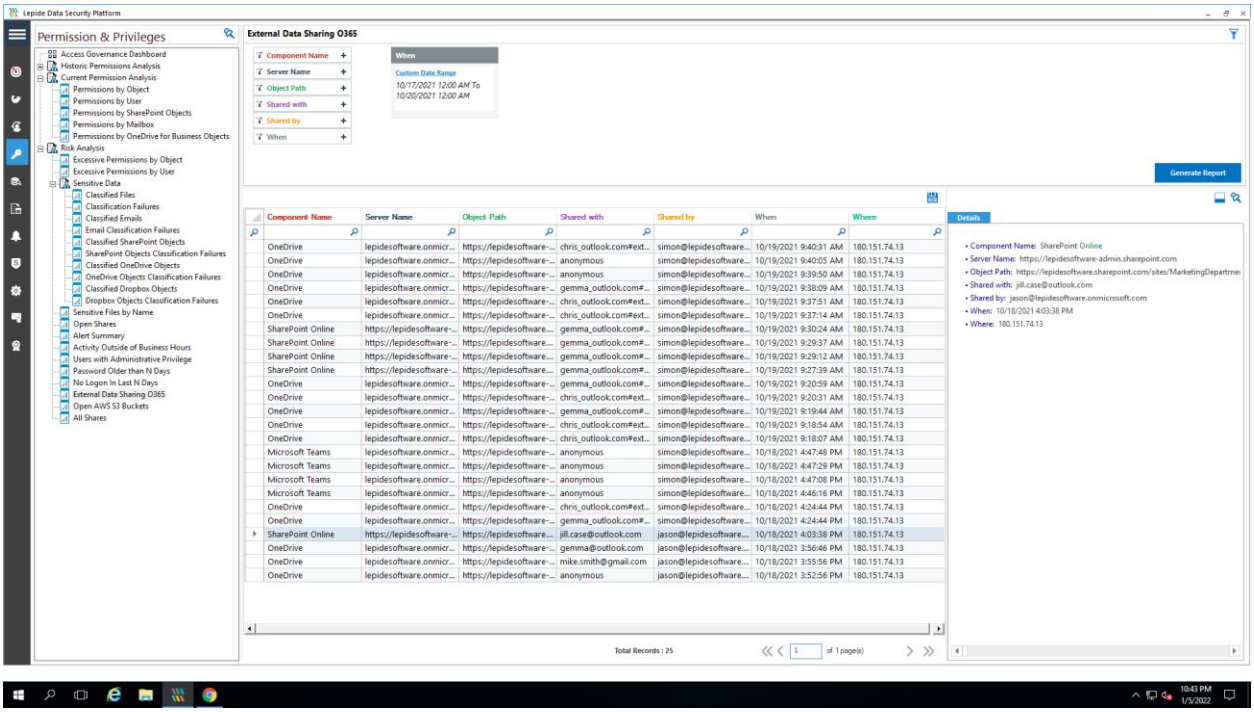

Figure 3: External Data Sharing 0365 Report with Data

The report shows all files that have been shared externally through Microsoft 365. The report can then be filtered, saved, or set to run on a pre-defined schedule.

5. Support

If you are facing any issues whilst installing, configuring or using the solution, you can connect with our team using the below contact information.

Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

6. Trademarks

Lepide Data Security Platform, Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.