



ALIGNMENT GUIDE

ALIGNING LEPIDE FOR

MICROSOFT 365

COPILOT

Table of Contents

1. Introduction.....	3
2. Aligning Lepide for Microsoft 365 Copilot	3
3. Lepide Core Capabilities	6
3.1. - Lepide Identify	6
3.2. - Lepide Trust	8
3.3. - Lepide Audit	9
3.4. - Lepide Detect.....	10
3.5. - Lepide Protect.....	11
4. Support	13
5. Trademarks	13

1. Introduction

Productivity within organizations can be improved by using AI tools, including Copilot, to enable better use of data and to provide additional methods of content creation.

However, many companies simply aren't ready to adopt AI due to major concerns about security and privacy. This is where Lepide comes in.

The Lepide Copilot Security Solution enables you to minimize your threat surface to avoid the unintentional exposing of sensitive information and keep your Microsoft 365 Copilot data secure. It includes predefined reports so that you can identify, classify and monitor all AI created data and detect and respond to any suspicious Copilot user behavior.











2. Aligning Lepide for Microsoft 365 Copilot

There are a number of key questions that you need to be able to answer to be able to align the Lepide Data Security Platform for M365 Copilot security.

In the table below, we align Lepide technology to these questions:

Phase	Actions to Take	Technology to Implement
<p>Pre-Deployment (reducing your threat surface to facilitate a secure deployment).</p>	<p>See who has access to sensitive data.</p>	<ul style="list-style-type: none">  Users with Admin Privileges Report (Lepide Trust)  Permissions by User Report (Lepide Trust)  Inactive Users Report (Lepide Audit)  Excessive Permissions by User Report (Lepide Trust)  Open Shares Report (Lepide Audit)  Data Classification (Lepide Identify)  Permissions Remediation (Lepide Protect)
	<p>Identify and revoke excessive permissions.</p>	<ul style="list-style-type: none">  Inactive Users Report (Lepide Audit)  Excessive Permissions by User Report (Lepide Trust)  Excessive Permissions by Object Report (Lepide Trust)  Permissions by User Report (Lepide Trust)  Users with Admin Privileges Report (Lepide Trust)  Open Shares Report (Lepide Trust)  Data Classification (Lepide Identify)  Permissions Remediation (Lepide Protect)  Remove Inactive Users (Lepide Protect)

	Clean up inactive users in Active Directory / Entra ID.	 Remove Inactive Users (Lepide Protect)
	Identify what sensitive data you have.	 Data Classification (Lepide Identify)  Classified Files Reports (Lepide Identify)  Classified Emails Reports (Lepide Identify)  Classified SharePoint Objects Reports (Lepide Identify)  Classified OneDrive Objects Reports (Lepide Identify)  Classified Dropbox Objects Reports (Lepide Identify)  Open Shares Report (Lepide Trust)
	Identify sensitive data open to all users.	 Open Shares Report (Lepide Trust)
	Identify users with non-compliant passwords.	 Users whose Password Never Expires Report (Lepide Trust)  Password Older than N Days (Lepide Trust)  User with Soon to Expire Password (Lepide Trust)  User with Expired Password (Lepide Trust)  Users with Change Password at Next Login (Lepide Trust)
	Identify stale data	 Stale Data Report (Lepide Trust)



		 Stale Data report for SharePoint Online Server (Lepide Trust)
Post Deployment (ensuring ongoing data protection whilst using Copilot)	Detect and respond to anomalous user behavior.	 Anomaly Analysis (Lepide Trust)
	Detect high-risk Copilot searches.	 All Copilot Searches (Lepide Trust)
	Monitor Copilot access.	 Copilot Access (Lepide Trust)  Copilot Access Changed (Lepide Trust)  Inactive Users with Copilot Access (Lepide Trust)  All Copilot Searches (Lepide Trust)  Sensitive Data Accessed by Copilot (Lepide Audit)  Sensitivity Label Changes (Lepide Audit)
	Identify inactive users with Copilot access.	 Inactive Users with Copilot Access (Lepide Trust)

3. Lepide Core Capabilities

3.1. - Lepide Identify

Automatically scan, discover and classify data at the point of creation to help you stay on top of where your sensitive data is located. Remove false positives with proximity scanning technology. This helps to improve the accuracy even further than most classification solutions. Categorize and score data based on compliance, risk, occurrence, monetary value, and more to stay on top of your most sensitive data.

Report
 Report Name - Classified Files
 Filters : File Server : [Equals (All)]
 Home / Lepide Identify / Reports / Classified Files

File Server	File Path	Content Type(s)	Compliance	Count	Risk Level	Monetary Value		Classification Date Time
DCD01	\\DCD01\Company Share\Fin...	SSN	GLBA	11	3223	\$ 6446		26-05-2023 01:27:12 PM
DCD01	\\DCD01\Company Share\Fin...	Phone Number ; Address	NPPI	51	14943	\$ 29886		26-05-2023 01:26:15 PM
DCD01	\\DCD01\Company Share\Fin...	Phone Number	NPPI	28	8204	\$ 16408		26-05-2023 01:25:36 PM
DCD01	\\DCD01\Company Share\Fin...	SSN	GLBA	26	7618	\$ 15236		26-05-2023 01:25:09 PM
DCD01	\\DCD01\Company Share\Fin...	Phone number ; Address	NPPI	50	14650	\$ 29300		26-05-2023 01:24:23 PM
DCD01	\\DCD01\Company Share\Fin...	Phone number	NPPI	27	7911	\$ 15622		26-05-2023 01:23:01 PM
DCD01	\\DCD01\Company Share\Fin...	SSN	GLBA	24	7032	\$ 14064		26-05-2023 01:22:19 PM
DCD01	\\DCD01\Company Share\Fin...	Address	NPPI	22	6446	\$ 12892		26-05-2023 01:21:51 PM
DCD01	\\DCD01\Company Share\Fin...	Phone Number ; Address	NPPI	44	12892	\$ 25784		26-05-2023 01:14:49 PM

Total Records - 213

First Previous 1 / 22 Next Last

10 / Page

In Summary:

- Discover and classify data in real Tag data.
- Data valuation.
- Identify data most at risk.

For More Information:

<https://www.lepide.com/lepide-identify/>

3.3. - Lepide Audit

Audit, report and alert on changes being made to sensitive data and your hybrid environment. Roll back unwanted changes and restore deleted objects to maintain system integrity. Track any changes and modifications users are making to critical files and folders.

Report

Report Name - All Environment Changes

Filters : Component Name : [Equals [Active Directory File Server Exchange Online]]

Home / Lepide Auditor / Reports / All Environment Changes

Oct 1, 2024 - Oct 1, 2024

Generate Report Export

Component Name	Server Name	Object Path	Object Type	Who	When	Operation	Content Type	Compliance	Risk Level	Monetary Value	What	Where	Criticality
Active Directory	lpde4.local	N/A	User	Neal Gamby	01-10-2024 08:58:2...	Login Attempt Failed	N/A	N/A	N/A	N/A	user name does no...	B_508	High
Active Directory	lpde4.local	N/A	User	Neal Gamby	01-10-2024 08:58:2...	Login Attempt Failed	N/A	N/A	N/A	N/A	user name does no...	B_508	High
Active Directory	lpde4.local	N/A	User	Neal Gamby	01-10-2024 08:58:2...	Login Attempt Failed	N/A	N/A	N/A	N/A	user name does no...	B_508	High
Active Directory	lpde4.local	N/A	User	Neal Gamby	01-10-2024 08:58:1...	Login Attempt Failed	N/A	N/A	N/A	N/A	user name does no...	B_508	High
Active Directory	lpde4.local	N/A	User	Neal Gamby	01-10-2024 08:58:1...	Login Attempt Failed	N/A	N/A	N/A	N/A	user name does no...	B_508	High
Active Directory	lpde4.local	N/A	User	Neal Gamby	01-10-2024 08:58:0...	Login Attempt Failed	N/A	N/A	N/A	N/A	user name does no...	B_508	High
Active Directory	lpde4.local	N/A	User	Neal Gamby	01-10-2024 08:58:0...	Login Attempt Failed	N/A	N/A	N/A	N/A	user name does no...	B_508	High
Active Directory	lpde4.local	N/A	User	Neal Gamby	01-10-2024 08:57:5...	Login Attempt Failed	N/A	N/A	N/A	N/A	user name does no...	B_508	High
Active Directory	lpde4.local	N/A	User	Neal Gamby	01-10-2024 08:57:5...	Login Attempt Failed	N/A	N/A	N/A	N/A	user name does no...	B_508	High

Total Records - 8974

First Previous 1 / 898 Next Last

10 / Page

In Summary:

- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

For More Information:

<https://www.lepide.com/lepideauditor/>

3.4. - Lepide Detect

Machine Learning backed anomaly spotting technology will allow you to determine when one of your users becomes an insider threat. Hundreds of threat models, tailored to specific data security threats, generate real time alerts when the security of your data is in jeopardy. Automated threat responses can be triggered to perform threat mitigations, such as shutting down an affected computer or server.

Report
 Report Name - Failed Logon
 Filters : Server Name : [Equals][All]

Home / Lepide Auditor / Reports / Active Directory / Failed Logon

Mar 26, 2024 - Mar 26, 2024 Generate Report Export

Server Name	Who	When	Where	Reason
lpde4.local	neal.gamby@lpde4.local	19-04-2024 6.10	DMD01	user name does not exist
lpde4.local	neal.gamby@lpde4.local	19-04-2024 6.10	DMD01	user name does not exist
lpde4.local	kelly.maxwell@lpde4.local	16-04-2024 22.20	DMD01	expired password
lpde4.local	kelly.maxwell	16-04-2024 22.20	DMD01	expired password
lpde4.local	kelly.maxwell	16-04-2024 22.20	DMD01	expired password
lpde4.local	kelly.maxwell	16-04-2024 22.20	DMD01	expired password
lpde4.local	kelly.maxwell	16-04-2024 22.20	DMD01	expired password
lpde4.local	LPDE4Kelly.Maxwell	15-04-2024 23.55	192.168.1.15	The user's password has expired.
lpde4.local	LPDE4Kelly.Maxwell	15-04-2024 23.55	192.168.1.15	The user's password has expired.

Total Reports : 50 First Previous 1 / 1 Next Last 50 / page

In Summary:

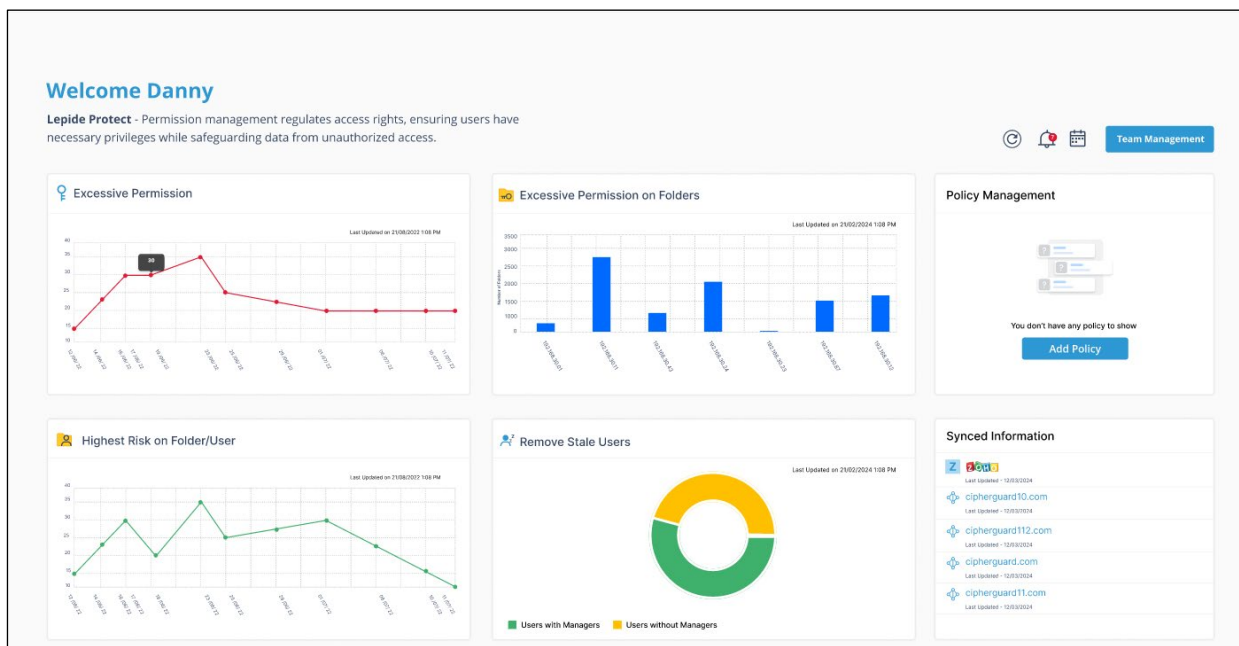
- Detect threats in real time with pre-defined threat models.
- Baseline/profile employee behavior.
- Identify anomalous employee behavior.
- Alert and respond to threats in real time.

For More Information:

<https://www.lepide.com/lepide-detect/>

3.5. - Lepide Protect

Reduce the complexity of managing user permissions. The permissions management system within Lepide Protect provides a straightforward and efficient way to manage permissions over all shared locations. It provides clear visibility as to who has access to what, including identifying excessive permissions. Once identified, excessive permissions can be revoked, and inactive users removed; permissions policies can be used to do this automatically.



In Summary:

- Identify and revoke excessive permissions.
- Remove inactive users to reduce your threat surface.
- Delegate permissions management to team leaders.
- Use policy management to automatically revoke permissions.

For More Information:

<https://www.lepide.com/lepide-protect/>

4. Support

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

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/>.

5. Trademarks

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.

