** Lepide

ALIGNMENT GUIDE

ALIGNING LEPIDE FOR DATA ACCESS GOVERNANCE

Table of Contents

1.	Introduction	3
2.	Aligning Lepide for Data Access Governance	3
3.	Lepide Core Capabilities	7
	3.1 Lepide Identify	7
	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

Data Access Governance (DAG) is the process of ensuring access is only in place based on those that need it and ensuring such access is checked and monitored thereafter. Also known as DAG, there are a whole separate category of solutions in the market for this problem, however, we have a very tangible solution that offers a lot of value to organizations with this objective.

Our solution helps organizations identify where their most sensitive data is, it shows them who has access, how that access was granted and what levels of access are held, along with insight as to how and when the privileges are being used - i.e. whether they are using the files they have access to.

Poor governance and insight around these areas leads to unnecessary risk from a security perspective. As we know Windows File Systems better than any other security vendor out there, we're able to deliver governance value in a way that other security vendors simply cannot do.

2. Aligning Lepide for Data Access Governance

There are a number of key questions that you need to be able to answer to be able to discover, govern and monitor data access.



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

Category	Actions to Take	Technology to implement
Discover	See when new sensitive data is created.	Oata Classification (Lepide Identify)
		Classified Emails Report (Lepide Identify)
		 Classified SharePoint Objects Report (<u>Lepide</u> Identify)
		Classified OneDrive Objects Report (<u>Lepide Identify</u>)



How to Align Lepide for Data Access Governance

		Ø (0) (0)	Classified DropBox Objects Report (Lepide Identify) Increased Threat Surface Area Threat Model (Lepide Detect) All Modifications in File Server Report (Lepide Audit)
Govern	See who has access to what.		Permissions by User Report (Lepide Trust) Inactive Users Report (Lepide Audit) Excessive Permissions by User Report (Lepide Trust) Users with Admin Privileges Report (Lepide Trust) Open Shares Report (Lepide Audit) Permissions by Object Report (Lepide Trust) Permissions Remediation (Lepide Protect) Remove Inactive Users (Lepide Protect)
	Work out the way in which the access was/is being granted. See when access to data was granted.		Permissions by User Report (Lepide Trust) Permissions by Object Report (Lepide Trust) Users with Admin Privileges Report (Lepide Trust) Permissions Modification Report – All Data Sources (Lepide Trust) Historical Permissions Analysis Reports (Lepide
	See users with access to sensitive data that is not being used.	Ø	Trust) Excessive Permissions by User Report (<u>Lepide Trust</u>)

How to Align Lepide for Data Access Governance

		8 •	Excessive Permissions by Object Report (<u>Lepide Trust</u>) Permissions Remediation (Lepide Protect)
Monitor	Detect when access to sensitive data changes.		Permissions Modification Report (Lepide Trust) Current Permissions Analysis Report (Lepide Trust) Historical Permissions Analysis Report (Lepide Trust) Any Permission Changes Threat Model (Lepide Detect)
	See where your most sensitive data is and why it's sensitive.	\$ \$ \$ \$ \$ \$	Data Classification (Lepide Identify)Classified Emails Report (Lepide Identify)Classified SharePoint Objects Report (Lepide Identify)Classified OneDrive Objects Report (Lepide Identify)Classified OneDrive Objects Report (Lepide Identify)
	Keep track of permission sprawl.		Excessive Permissions by User Report (Lepide Trust) Excessive Permissions by Object Report (Lepide Trust) Users with Admin Privileges Report (Lepide Trust) Historical Permissions Analysis Report (Lepide Trust) Permissions by User Report (Lepide Trust)

How to Align Lepide for Data Access Governance

	Ø	Permissions by Object Report (<u>Lepide Trust</u>)
	¢	Permissions Escalation (Groups) Threat Model (<u>Lepide Detect</u>)
	¢	Permissions Escalation (File) Threat Model (<u>Lepide</u> <u>Detect</u>)
	¢	Permissions Escalation (Folder) Threat Model (<u>Lepide Detect</u>)
	Q	Permissions Modification Report – All Data Sources (<u>Lepide Audit</u>)
		Permissions Remediation (Lepide Protect)
See how users are utilizing the access they've been given to the data.	Ø	Excessive Permissions by User Report (<u>Lepide Trust</u>)
	Ø	Excessive Permissions by Object Report (<u>Lepide Trust</u>)
	Ø	External Data Sharing for O365 Report (<u>Lepide Trust</u>)
	0	All Modifications in File Server Report – All Data Sources (<u>Lepide Audit</u>)

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 - Class	ified Files											
ilters : Server Name :										_		
Home / Lepdie Audit	tor / Report	ts / File Server / Classified Files							7	Ge	nerate Report	Export
File Server	\uparrow	File Path	↑ Content	Type(s)	\uparrow	Compliance 个	Count 🕆	Risk Level	Monetary Value	<u>۲</u>	R	↑ Cl
	Q		Q		Q	Q	Q	Q		Q		Q
DCD01		C:Company ShareFinancial Service	sF Credit C	ird - Amex Card		Payment Card Industry Data Securit	1	1	\$ 1	N	0	16
DCD01		C:Company ShareFinancial Service	sF Credit C	rd - Amex Card		Payment Card Industry Data Securit	1	1	S 1	N	0	16
DCD01		C:Company ShareFinancial Service	sF Credit C	rd - Diners Club		Payment Card Industry Data Securit	7	7	\$ 7	N	0	16
DCD01		C:Company ShareFinancial Service	sF Credit C	rd - Discover		Payment Card Industry Data Securit	1	1	\$ 1	N	0	16
DCD01		C:Company ShareFinancial Service	sF Credit C	rd - Amex Card		Payment Card Industry Data Securit	190	190	\$ 190	N	0	16
DCD01		C:Company ShareFinancial Service	sF Credit C	rd - Amex Card		Payment Card Industry Data Securit	5	5	\$ 5	N	0	16
DCD01		C:Company ShareFinancial Service	sF UK Posta	l Code		UK - GDPR	17	17	\$ 17	N	0	16
DCD01		C:Company ShareFinancial Service	sF Credit C	rd - Master		Payment Card Industry Data Securit	2	2	\$ 2	N	0	16
DCD01		C:Company ShareFinancial Service	sF Credit C	rd - Master		Payment Card Industry Data Securit	2	2	\$ 2	N	0	16
Total Reports : 50		-				First Previous 1	/ 1 Next Last				50 / 0	oage 🗸

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/



3.2. - Lepide Trust

Report on who has access to your most sensitive data and how they were granted that access. Specific reports for users with excessive permissions enable you to spot which users are most likely to be insider threats. Maintain your zero-trust policy by spotting when permissions change and reversing them.

port Name - Excessive Permissions by Use	r																				
rs : Component Name : [Equals [All]] AND e / Lepide Trust / Reports / Excessive F															-		Gener	ate Rep	ort	В	xpor
<< < 1 of 3 ► ₩	Server Name	Object Name	කී	6	Path	Owner	Last Scan	Last Modified	٩	•	Ð	<u>8</u>	Ø	Đ		D		۲	0	0	b
192.168.20.193	9		2		9	. a	Q	۱. Q													
Ipde4	DCD01	All Services	තී		C:VAll Services	Ipde4\Kelly.Maxwell	6/6/2023 4:33:55 PM	5/25/2023 3:12:46 PM	~	~	~	~	×	~	×	~	~	~	~	~	•
SA51000-C70NF2LB8OE8	DCD01	Budget Forecast	ස්	6	C:\Budget Forecast	Ipde4\Roy.Petty	6/7/2023 3:55:35 PM	3/15/2023 5:04:39 AM	~	~	~	~	~	~	~	~	~	~	~	~	
Administrator	DCD01	Company Share	සී	6	C:\Company Share	Ipde4\Administrator	6/7/2023 3:55:35 PM	5/11/2023 3:48:07 AM	~	~	~	~	~	~	~	~	~	~	~	~	
Akash	DCD01	Confidential files	ස්		C:\Confidential files	Ipde4\Roy.Petty	6/6/2023 4:33:55 PM	5/25/2023 3:12:28 PM	~	~	~	~	~	~	~	~	~	~	~	~	
Ash.Williams	DCD01	Employee's Accoun	ස්		C:\Employee's Account details	lpde4\Marty.Byrde	6/6/2023 4:33:55 PM	5/25/2023 3:12:41 PM	~	~	~	~	~	~	~	~	~	~	~	~	۰.
Bill		-																			
Developer-Ext	DCD01	Foreign designs	කී		C:\Foreign designs	Ipde4\Marty.Byrde	6/6/2023 4:33:55 PM	5/25/2023 3:12:37 PM	× .	× .	× .	× .	~	× .	× .	× .	× .	× .	~	× .	
Disaster.Dina	DCD01	Module Analysis Da	සී		C:\Module Analysis Data	Ipde4\Ethan.Hunt	6/6/2023 4:33:55 PM	5/25/2023 3:12:10 PM	~	~	~	~	~	~	~	~	~	~	~	~	
(2) Ethan.Hunt	DCD01	Project Details	:8:		C:\Proiect Details	lode4\Ethan.Hunt	6/6/2023 4:33:55 PM	5/25/2023 3:12:25 PM	1	1	~	1	1	~	1	1	1	1	~	1	
Guest	Name	ක් බ ක	Conte	nt Type		Monetary Value	Risk Level														
(1) Hank.Shrader		9			9	Q															

In Summary:

- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

For More Information:

https://www.lepide.com/lepide-trust/



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.

ome / Lepide Au	iditor / Reports / A	I Environment Chang	25								🔁 🗇 Oct 1, :	2024 - Oct 1, 2024 💌	Generate Repo	rt Export
Component Name	1 Server Name	↑ Object Path	↑ o	bject Type 🛛 🕆	Who 1	When 个	Operation 1	Content Type 1	Compliance 1	Risk Level 🔶 🕆	Monetary 1	What \uparrow	Where \uparrow	Criticality
	۹	Q	Q	Q		۱ <u>۹</u>	Q	Q	Q	٩	Q	Q	Q	
ctive Directory	Ipde4.local	N/A	U	ser	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	Ipde4.local	N/A	U	ser	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
ctive Directory	Ipde4.local	N/A	U	ser	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
ctive Directory	Ipde4.local	N/A	U	ser	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	Ipde4.local	N/A	Us	ser	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	Ipde4.local	N/A	U	ser	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	Ipde4.local	N/A	U	ser	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	Ipde4.local	N/A	U	ser	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
ctive Directory	Ipde4.local	N/A	Us	ser	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	Ipde4.local	N/A	Us	ser	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 - 8	1974					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 / Lepdie Auditor / Reports	s / Active Directory / Fa	ailed Logon			7	🛗 Mar 26, 2024 - Mar	r 26, 2024 💌 Generate	Report Export
Server Name		Who	Ŷ	When 个	Where	Ŷ	Reason	\uparrow
	Q		Q	c	t	Q		Q
Ipde4.local		neal.gamby@lpde4.local		19-04-2024 6.10	DMD01		user name does not exist	
Ipde4.local		neal.gamby@lpde4.local		19-04-2024 6.10	DMD01		user name does not exist	
Ipde4.local		kelly.maxwell@lpde4.local		16-04-2024 22.20	DMD01		expired password	
Ipde4.local		kelly.maxwell		16-04-2024 22.20	DMD01		expired password	
Ipde4.local		kelly.maxwell		16-04-2024 22.20	DMD01		expired password	
Ipde4.local		kelly.maxwell		16-04-2024 22.20	DMD01		expired password	
Ipde4.local		kelly.maxwell		16-04-2024 22.20	DMD01		expired password	
Ipde4.local		LPDE4Kelly.Maxwell		15-04-2024 23.55	192.168.1.15		The user's password has expire	ed.
Ipde4.local		LPDE4Kelly.Maxwell		15-04-2024 23.55	192.168.1.15		The user's password has expire	ed.
					0000000 COLO			
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.

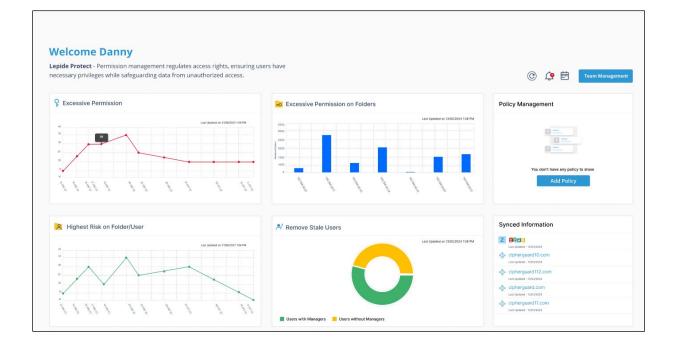
For More Information:

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 <u>https://www.lepide.com/contactus.html</u> 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.

