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.	Data Classification (Lepide Identify) Classified Emails Report (Lepide Identify) Classified SharePoint Objects Report (Lepide Identify) Classified OneDrive Objects Report (Lepide Identify)

		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.	Permissions by User Report (Lepide Trust) Permissions by Object Report (Lepide Trust) Users with Admin Privileges Report (Lepide Trust)
	See when access to data was granted.	Permissions Modification Report – All Data Sources (Lepide Trust) Historical Permissions Analysis Reports (Lepide Trust)
	See users with access to sensitive data that is not being used.	Excessive Permissions by User Report (Lepide Trust)

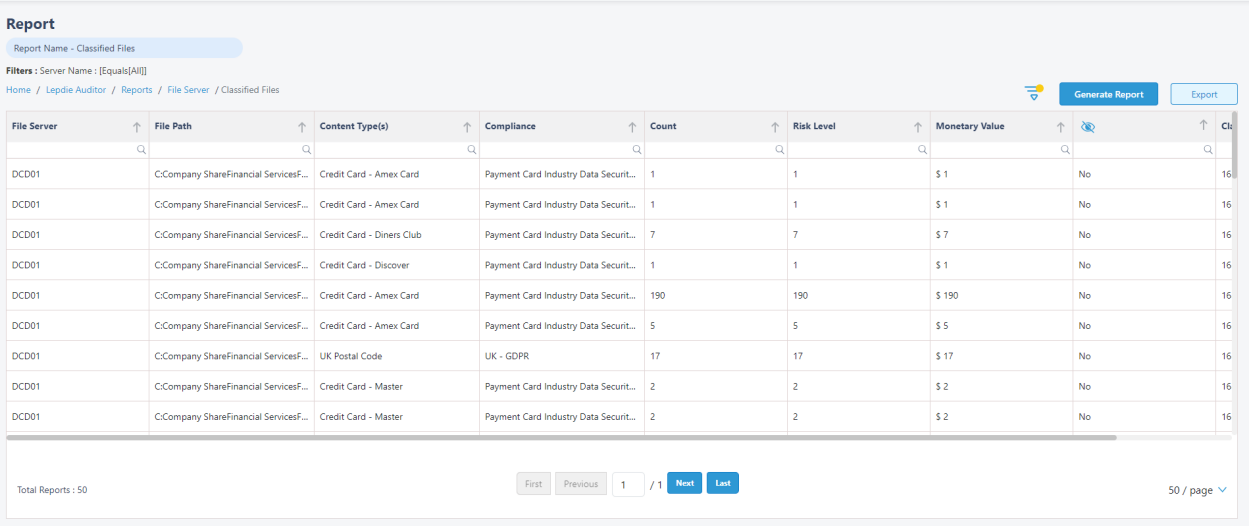
		Excessive Permissions by Object Report (Lepide Trust) Permissions Remediation (Lepide Protect)
Monitor	Detect when access to sensitive data changes.	Permissions Modification Report (Lepide Trust) Current Permissions Analysis Report (Lepide Trust) Historical Permissions Analysis Report (Lepide Trust) 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 DropBox 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)

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

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.



In Summary:

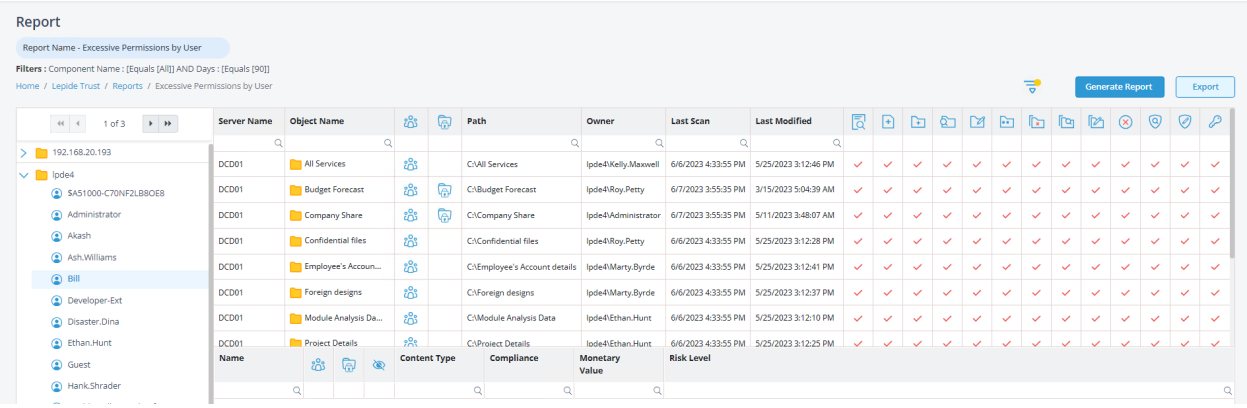
- Discover and classify data in real Tag data.
- Data valuation.
- Identify data most at risk.

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.



In Summary:

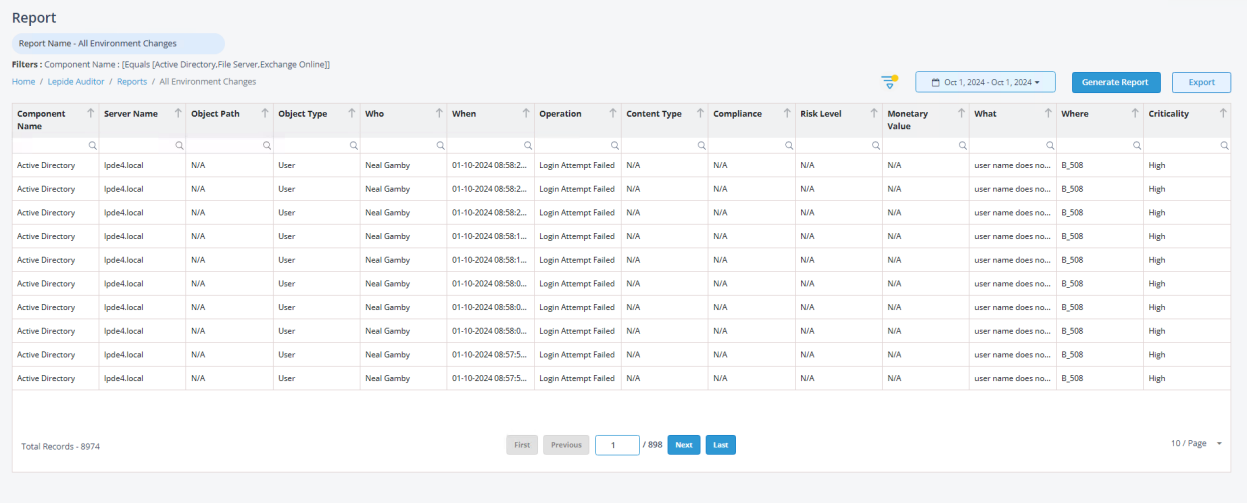
- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

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.



In Summary:

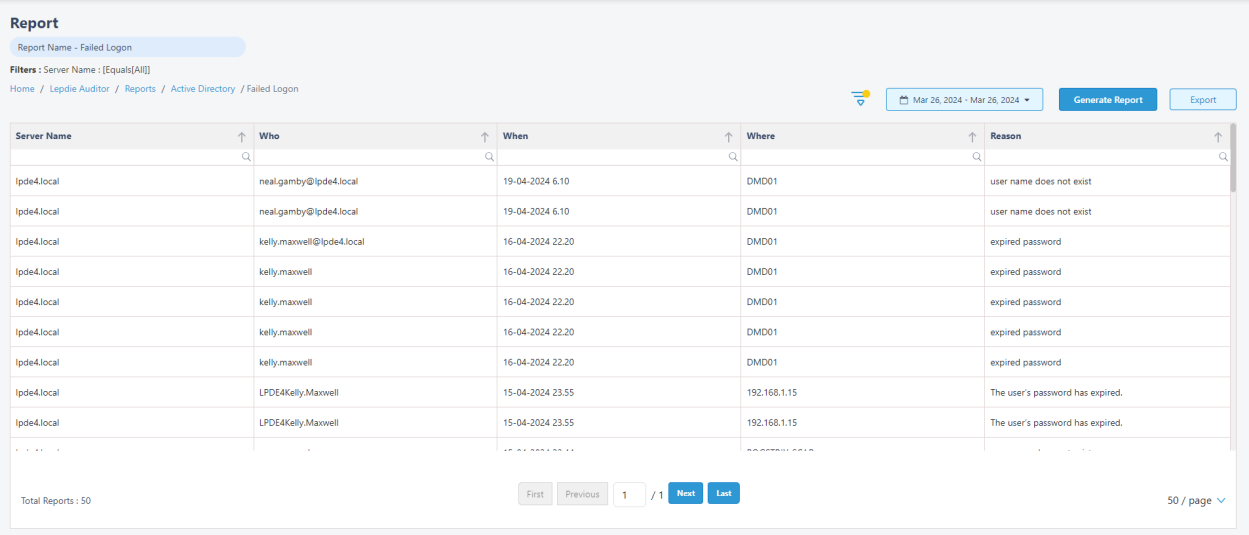
- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

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.



In Summary:

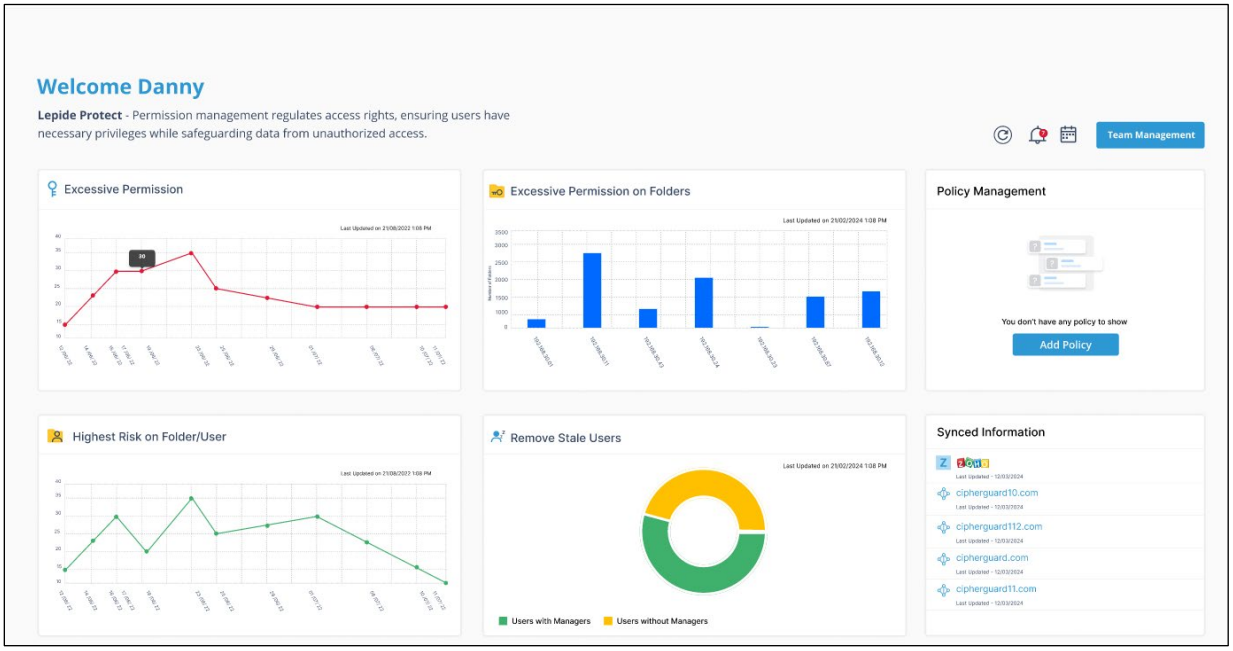
- Detect threats in real time with pre-defined threat models.
- Baseline/profile employee behavior.
- Identify anomalous employee behavior.
- Alert and respond to threats in real time.

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.