Lepide

ALIGNMENT GUIDE

ALIGNING LEPIDE FOR PRIVILEGED ACCESS MANAGEMENT

Table of Contents

1. Introduction

Privileged Access Management (PAM) is a huge priority right now and is cited by Gartner as a top 5 spending priority. Also referred to as PAM, it is a component of Identity and Access Management (IAM) that is designed to manage and monitor privileged access to accounts and applications, alerting system administrators to high-risk events.

PAM vendors are typically not strong at providing alerts or insights around what their privileged users are doing within or to Active Directory (AD) (i.e. they don't track changes or events made by privileged users). They also rarely have any insight into what's happening at a data level (i.e. an inability to understand sensitive unstructured data stored on Windows File Servers or Microsoft 365). So once a privileged user is authenticated and is inside the network, the value of a PAM solution diminishes.

The other challenge of PAM is that solutions nearly all rely heavily on synchronization with Active Directory. So, if the Active Directory is not in an appropriate state, the problem replicates across. For example, if you don't have the right levels of access or if the schema is not right in your Active Directory then it won't be right within your PAM deployment. Any organization with an initiative for PAM should deploy a solution like Lepide to ensure the integrity of the Active Directory in advance, and in parallel, to ensure a successful deployment.

2. Aligning Lepide for Privileged Access Management

There are a number of key questions that you need to be able to answer to be able to secure data, analyze user behavior and govern data access.

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

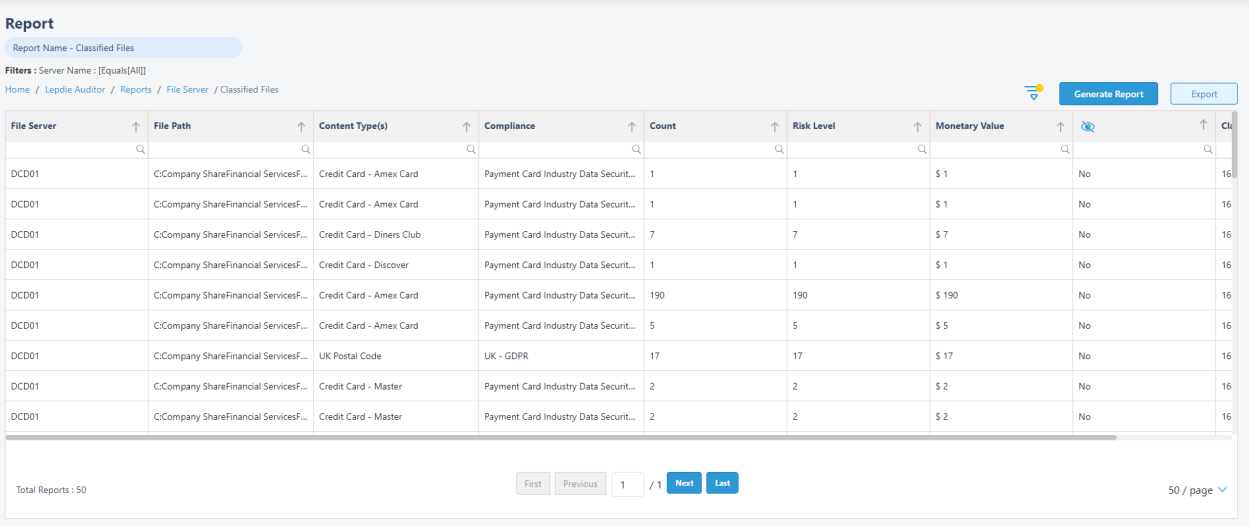
Category	Actions to Take	Technology to implement
Security States	Identify passwords in Active Directory that are set to never expire.	Users whose Password Never Expires Report (Lepide Audit)
	Get a list of all your domain admins in Active Directory.	Users with Admin Privileges Report (Lepide Trust)
	Roll back changes made in error in your Active Directory by IT Admins.	Active Directory Restore (Lepide Audit)
User Behavior Analytics	Keep track of what your most privileged users are doing in your Active Directory.	Users with Admin Privileges Report (Lepide Trust) Permissions Escalation Threat Model (Groups) (Lepide Detect) All Modifications in Active Directory Report (Lepide Audit)
	Spot privilege abuse or misuse around your Active Directory or Windows File Systems.	Permissions Escalation (Groups) Threat Model (Lepide Detect) Permissions Escalation (File) Threat Model (Lepide Detect) Permissions Escalation (Folder) Threat Model (Lepide Detect) All Modification Reports – All Systems and Platforms (Lepide Audit) All Environment Changes Report (Lepide Audit) Anomaly Spotting (Lepide Detect) Activity Outside of Business Hours Report (Lepide Audit)

	Get an audit trail of all activity across your systems and data around your privileged users.	All Environment Changes Report (Lepide Audit)
Access Governance	Ensure you keep your Active Directory clean in terms of joiners, movers, and leavers.	Inactive Users Report (Lepide Audit) Active Directory Cleaner (Lepide Audit) Remove Inactive Users (Lepide Protect)
	Identify privileged users with excessive permissions	Excessive Permissions by User Report (Lepide Trust) Excessive Permissions by Object Report (Lepide Trust) Permissions Remediation (Lepide Protect)
	See the means in which permissions are being granted including nested security groups	Permissions by User Report (Lepide Trust) Permissions by Object Report ((Lepide Trust)
	Visibility when changes are made to your most privileged user accounts.	All Modifications in Active Directory Report (Lepide Audit) Permissions Escalation Threat Model (Groups) (Lepide Detect)
	See your most privileged users in terms of their access to your most sensitive data.	Users with Admin Privileges Report ((Lepide Trust) Permissions by User Report (Lepide Trust) Permissions by Object Report (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.



In Summary:

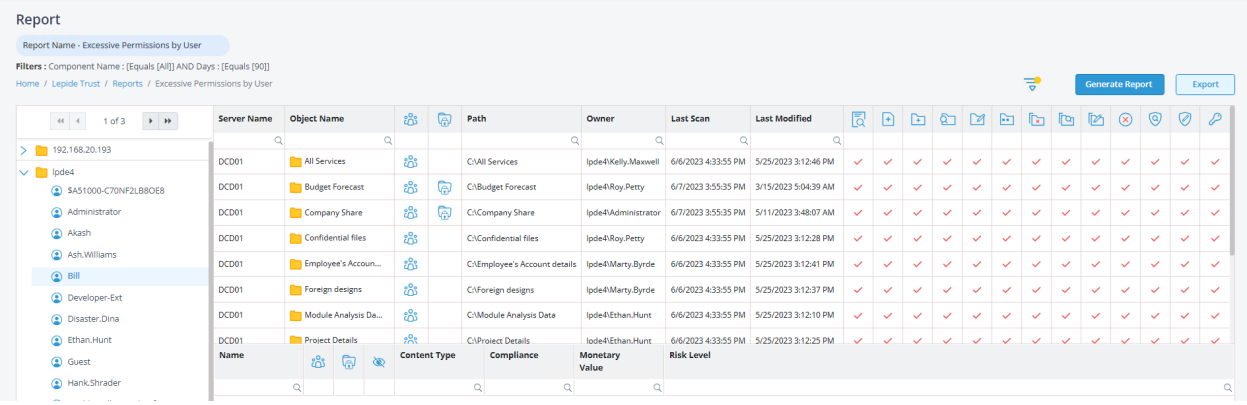
- Discover and classify data in real Tag data.
- Data valuation.
- Identify data most at risk.

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:

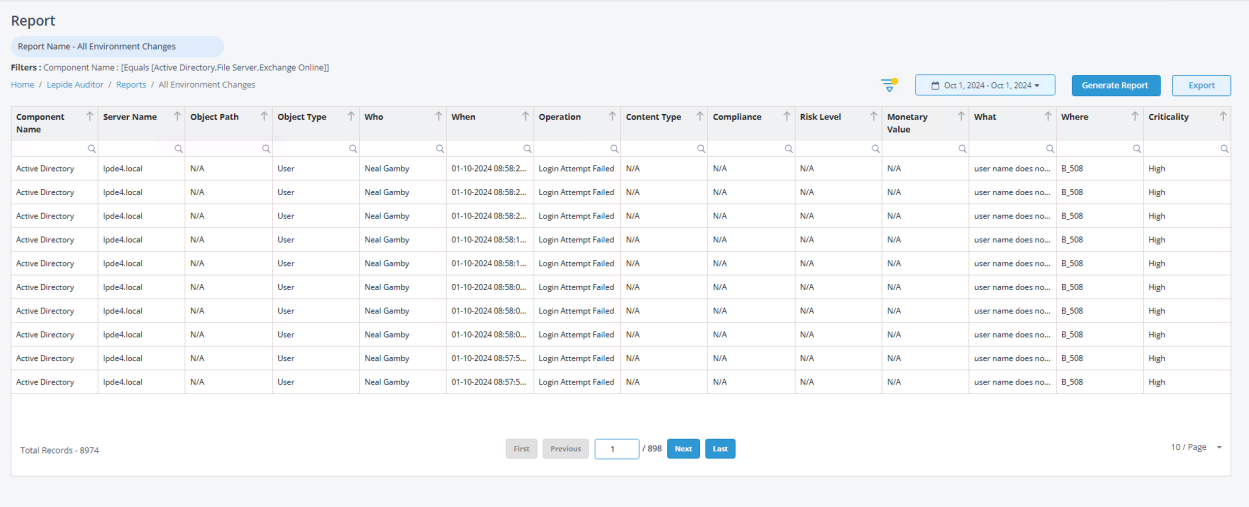
- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

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:

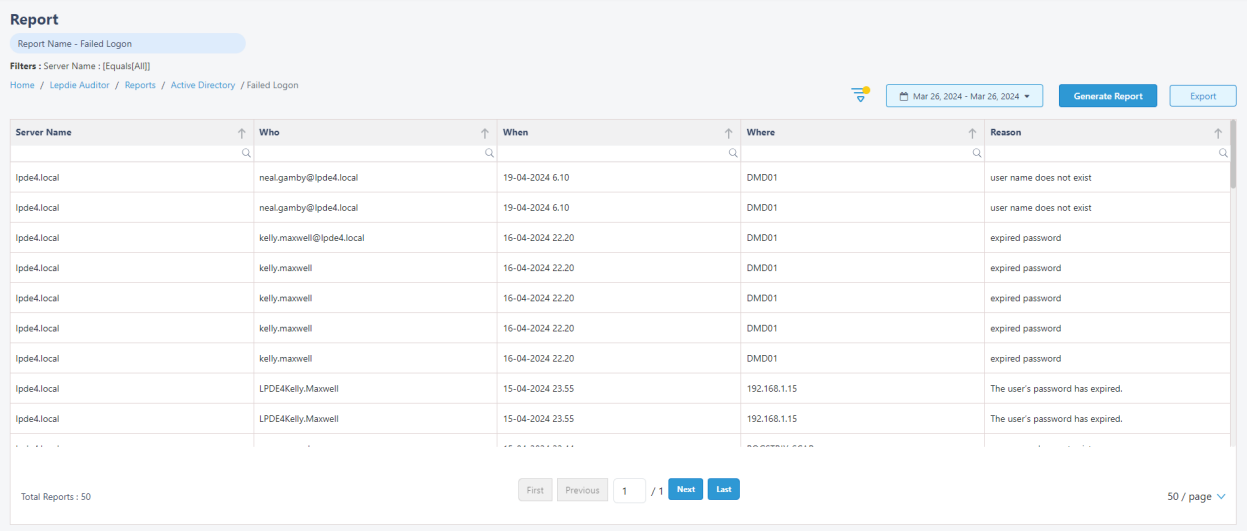
- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

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:

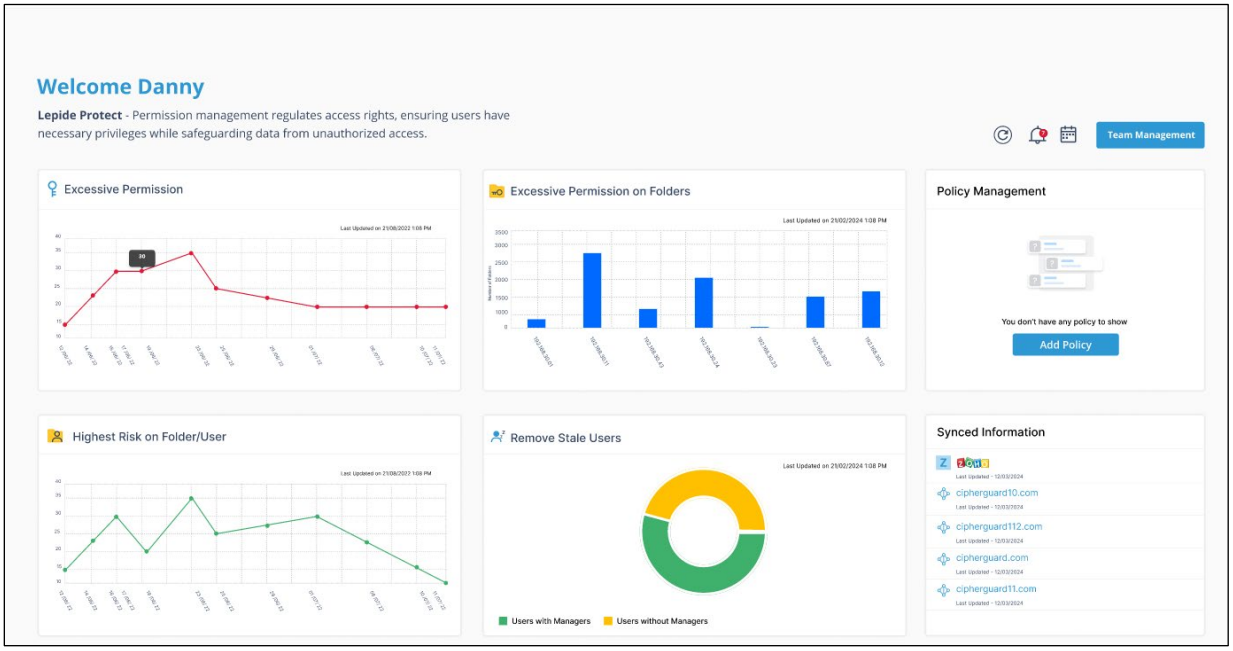
- Detect threats in real time with pre-defined threat models.
- Baseline/profile employee behavior.
- Identify anomalous employee behavior.
- Alert and respond to threats in real time.

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.