Lepide

ENABLEMENT GUIDE

ENABLING LEPIDE FOR A

DATA BREACH

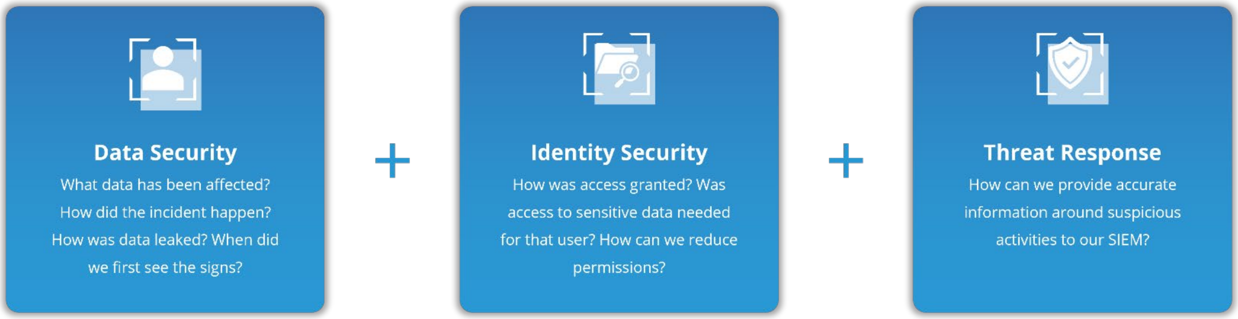
Table of Contents

1. Introduction

A data breach is a security violation where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by someone who does not have the authorization to do so, ie unintended or inappropriate disclosure of corporate data. In 2021 there were 5250 confirmed data breaches reported, however this is likely to be only 10% of the total number as most go unreported. Breaches on average cost an organization $4.6 Mn in fines, not to mention the intangible damage to reputation or brand. Many data breaches are preventable and a solution like ours enables organizations to take measures to prevent, detect and respond to breaches significantly faster than other security vendors. Our in-depth knowledge of Active Directory, Windows File Servers and Office 365 enables us to deliver value in a way no other security vendor can. We empower security teams with a unique set of tools to detect breaches earlier and run fast, accurate investigations.

2. Aligning Lepide for a Data Breach

There are a number of key questions that you need to be able to answer to be able to secure your data, identify, and respond to a data breach.



Data Security
What data has been affected? How did the incident happen? How was data leaked? When did we first see the signs?

+

Identity Security
How was access granted? Was access to sensitive data needed for that user? How can we reduce permissions?

+

Threat Response
How can we provide accurate information around suspicious activities to our SIEM?

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

Category	Actions to Take	Technology to implement
Data Security	How to see what sensitive data has been affected by the incident or breach.	All Modifications in File Server Report (Lepide Audit) Files Renamed Report (Lepide Audit) Read Failed Report (Lepide Audit)

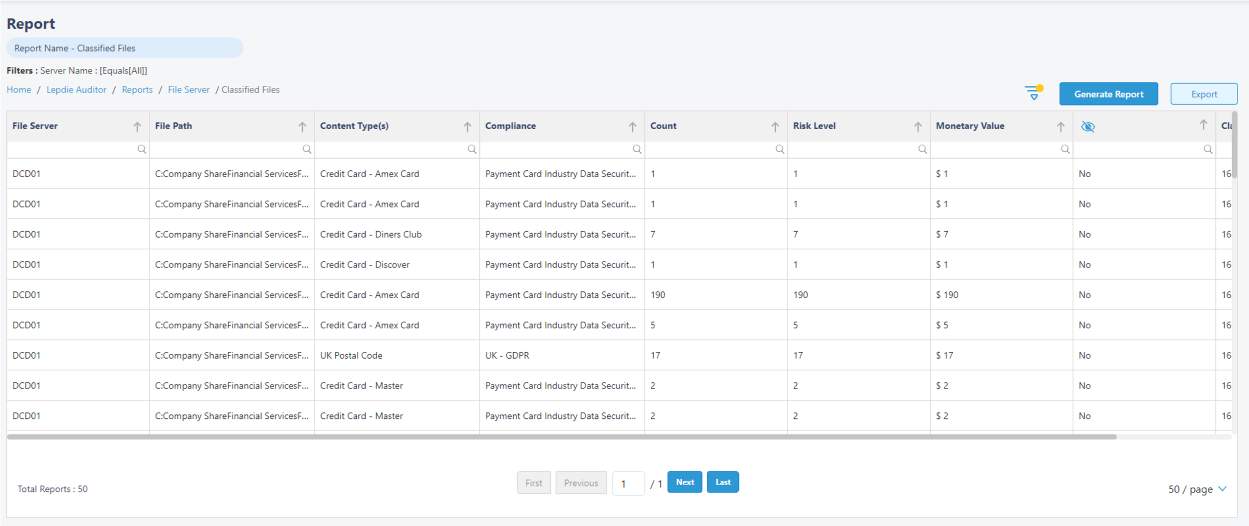
		All Environment Changes Report (Lepide Audit) Sensitive Data Classification (Lepide Identify)
	How the data was shared or leaked.	External Data Sharing 0365 Report (Lepide Audit) File Copied Report (Lepide Audit) Classified Emails Report (Lepide Audit) Mailbox Accessed by Non-owners Report (Lepide Audit)
	How to see the first signs of an incident that lead to a breach.	All Modifications in File Server Report (Lepide Audit) Anomaly Spotting (Lepide Detect) **Any** Threat Model Triggered (Lepide Detect)
	How the incident started and how it spread.	All Modifications in File Server Report (Lepide Audit) Potential Ransomware Attack Threat Model (Lepide Detect) Files Renamed Report (Lepide Audit) Read Failed Report (Lepide Audit) All Permissions Modifications Report (File Server) (Lepide Trust)
Identity Management	How the source of the breach gained access.	All Environment Changes Report (Lepide Identify) Permissions by User Report (Lepide Trust)

	Reduce permissions to sensitive data to reduce the impact of a breach.	Inactive Users Report (Lepide Audit) Excessive Permissions by User 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) Remove Inactive Users (Lepide Protect)
	Identify which users were compromised in the incident. Finding out what else they have access to.	Permissions By Object Report (Lepide Trust) Permissions by User Report (Lepide Trust)
	Whether the breach was due to human error, a compromised user account or rogue employee.	All Modifications in File Server Report (Lepide Audit) Permissions by User Report (Lepide Trust)
Response	Providing accurate information around suspicious activities to our SIEM.	SIEM Integration (Lepide Detect)

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 : Server Name : [Equals[All]]

Home / Lepdie Auditor / Reports / File Server / Classified Files

File Server	File Path	Content Type(s)	Compliance	Count	Risk Level	Monetary Value		Cl
DCD01	C:Company ShareFinancial ServicesF...	Credit Card - Amex Card	Payment Card Industry Data Securit...	1	1	$ 1	No	16
DCD01	C:Company ShareFinancial ServicesF...	Credit Card - Amex Card	Payment Card Industry Data Securit...	1	1	$ 1	No	16
DCD01	C:Company ShareFinancial ServicesF...	Credit Card - Diners Club	Payment Card Industry Data Securit...	7	7	$ 7	No	16
DCD01	C:Company ShareFinancial ServicesF...	Credit Card - Discover	Payment Card Industry Data Securit...	1	1	$ 1	No	16
DCD01	C:Company ShareFinancial ServicesF...	Credit Card - Amex Card	Payment Card Industry Data Securit...	190	190	$ 190	No	16
DCD01	C:Company ShareFinancial ServicesF...	Credit Card - Amex Card	Payment Card Industry Data Securit...	5	5	$ 5	No	16
DCD01	C:Company ShareFinancial ServicesF...	UK Postal Code	UK - GDPR	17	17	$ 17	No	16
DCD01	C:Company ShareFinancial ServicesF...	Credit Card - Master	Payment Card Industry Data Securit...	2	2	$ 2	No	16
DCD01	C:Company ShareFinancial ServicesF...	Credit Card - Master	Payment Card Industry Data Securit...	2	2	$ 2	No	16

Total Reports : 50

In Summary:

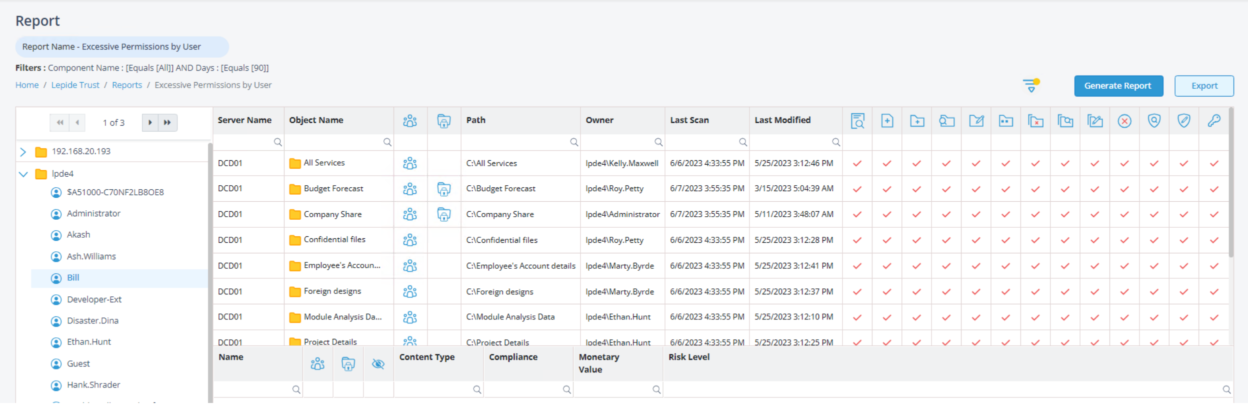
- Discover and classify data in real Tag data.
- Data valuation.
- Identify data most at risk.

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.



Report

Report Name - Excessive Permissions by User

Filters : Component Name : [Equals [All]] AND Days : [Equals [90]]

Home / Lepide Trust / Reports / Excessive Permissions by User

- 192.168.20.193
- lpde4
  - $A51000-C70NF2LB8OE8
  - Administrator
  - Akash
  - Ash.Williams
  - Bill
  - Developer-Ext
  - Disaster.Dina
  - Ethan.Hunt
  - Guest
  - Hank.Shrader

Server Name	Object Name	👥	🔒	Path	Owner	Last Scan	Last Modified													
DCD01	All Services	👥		C:\All Services	lpde4\Kelly.Maxwell	6/6/2023 4:33:55 PM	5/25/2023 3:12:46 PM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Budget Forecast	👥	🔒	C:\Budget Forecast	lpde4\Roy.Petty	6/7/2023 3:55:35 PM	3/15/2023 5:04:39 AM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Company Share	👥	🔒	C:\Company Share	lpde4\Administrator	6/7/2023 3:55:35 PM	5/11/2023 3:48:07 AM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Confidential files	👥		C:\Confidential files	lpde4\Roy.Petty	6/6/2023 4:33:55 PM	5/25/2023 3:12:28 PM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Employee's Accoun...	👥		C:\Employee's Account details	lpde4\Marty.Byrde	6/6/2023 4:33:55 PM	5/25/2023 3:12:41 PM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Foreign designs	👥		C:\Foreign designs	lpde4\Marty.Byrde	6/6/2023 4:33:55 PM	5/25/2023 3:12:37 PM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Module Analysis Da...	👥		C:\Module Analysis Data	lpde4\Ethan.Hunt	6/6/2023 4:33:55 PM	5/25/2023 3:12:10 PM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Project Details	👥		C:\Project Details	lpde4\Ethan.Hunt	6/6/2023 4:33:55 PM	5/25/2023 3:12:25 PM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Name	👥	🔒		Content Type	Compliance	Monetary Value	Risk Level

In Summary:

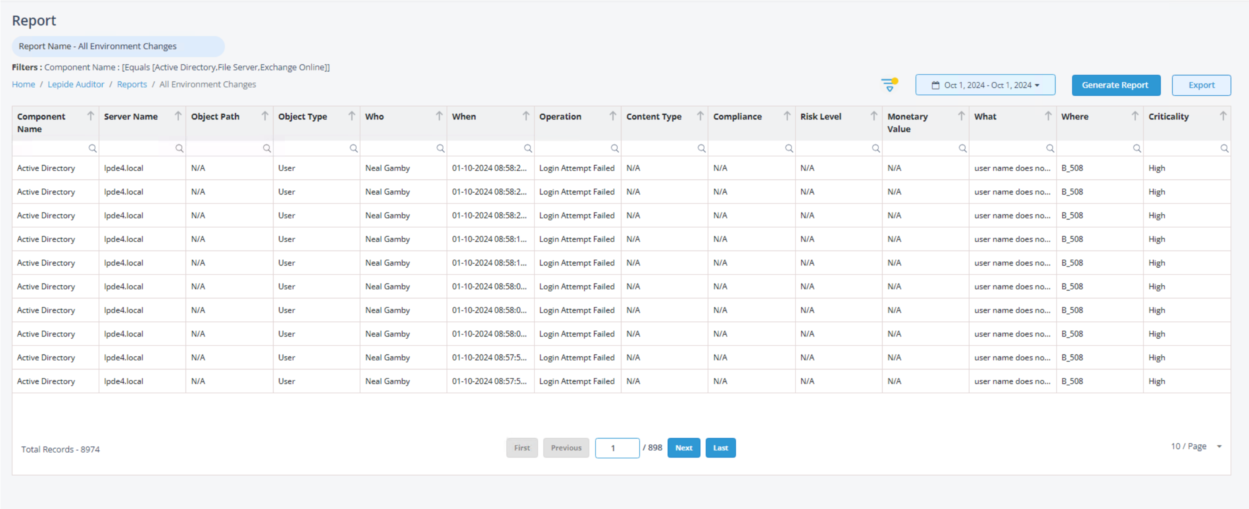
- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

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.



Report

Report Name - All Environment Changes

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

Home / Lepide Auditor / Reports / All Environment Changes

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 08:58:0...	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

In Summary:

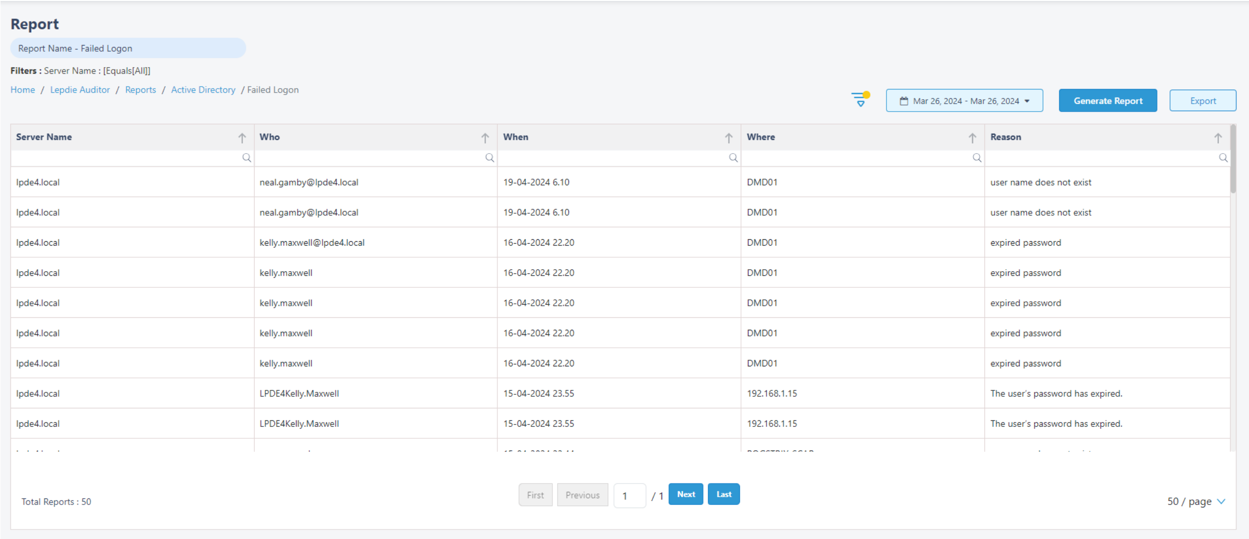
- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

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 / Active Directory / Failed Logon

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

In Summary:

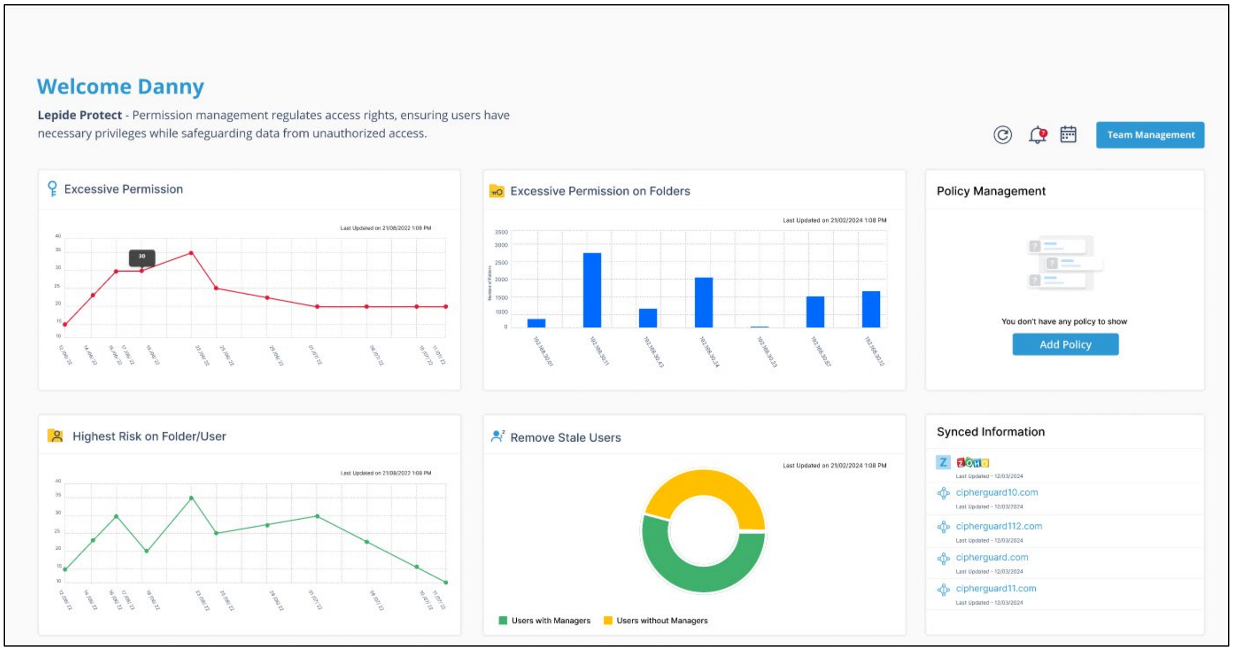
- Detect threats in real time with pre-defined threat models.
- Baseline/profile employee behavior.
- Identify anomalous employee behavior.
- Alert and respond to threats in real time.

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.



Welcome Danny

Lepide Protect - Permission management regulates access rights, ensuring users have necessary privileges while safeguarding data from unauthorized access.

You don't have any policy to show

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.