Lepide

ENABLEMENT GUIDE

ENABLING LEPIDE FOR

COMPLIANCE

Table of Contents

1. Introduction

Compliance is a huge problem for organizations and is a problem that is set to get tougher in years to come with more and more regulation coming into play and existing regulations being more stringently enforced. By the end of 2023, modern privacy laws will cover the personal information of 75% of the world's population.

Security teams are plagued with requests from the business to provide audit reports to prove they are taking the necessary steps to ensure they're compliant.

The depth of knowledge we have around core windows infrastructure along with how and where regulated data is stored and used places us in a unique position to enable organizations to meet their compliance objectives. Without our solution these common compliance questions are incredibly difficult, if not impossible, for organizations to answer.

2. Aligning Lepide for Compliance

There are a number of key questions that you need to be able to answer to be able to protect data and meet compliance regulations.

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

Category	Actions to Take	Technology to implement
Data Protection	Ensure that employees only have access to data they need. Reduce sprawl.	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 Audit) Data Classification (Lepide Identify) Increased Threat Surface Area Threat Model (Lepide Detect)

		Permissions Escalation (Groups) Threat Model (Lepide Detect) Permissions Escalation (File) Threat Model (Lepide Detect) Permissions Escalation (Folder) Threat Model (Lepide Detect)
	Manage inactive user accounts in Active Directory.	Inactive Users Report (Lepide Audit) Active Directory Cleaner (Lepide Audit)
	Get an audit report of what employees are doing with regulated data.	Classified Emails Report (Lepide Identify) Classified SharePoint Objects Report (Lepide Identify) Classified OneDrive Objects Report (Lepide Identify) Classified DropBox Objects Report (Lepide Identify) All Environment Changes Report (Lepide Audit) All Data Interation Reports for File Server, SharePoint, SharePoint Online, OneDrive (Lepide Audit) All Mailbox Access Reports (Lepide Audit)

	Handle joiners, movers, and leavers to maintain appropriate access.	Permissions by User Report (Lepide Trust) Historical Permissions Report (Lepide Trust) Excessive Permissions by Object Report (Lepide Trust) Inactive Users Report (Lepide Audit) Users with Admin Privileges Report (Lepide Trust)
	See who has privileged access to Active Directory.	Users with Admin Privileges Report (Lepide Trust) Active Directory Permissions Reports (Lepide Trust)
	See when employees are logging on to the corporate network via Active Directory.	Activity Outside of Business Hours Report (Lepide Audit) Logon/Logoff Auditing (Lepide Audit) Failed Logon Report (Lepide Audit) Sucessful User Logon/Logoff Report (Lepide Audit) User Logged on Multiple Computers Report (Lepide Audit) Concurrent Logons Report (Lepide Audit) Domain Controller Logon/Logoff Report (Lepide Audit) Potential Brute Force Attack Threat Model (Lepide Detect)

	See what changes are being made to Active Directory. Get an audit trail.	Active Directory Modification Reports (Lepide Audit) Historic Permissions – Active Directory Analysis Reports (Lepide Trust) Permissions by User Report (Lepide Trust)
	Keep track of changes to group memberships and group policies.	Group Policy Object Created Report (Lepide Audit) Group Policy Object Deleted Report (Lepide Audit) Group Policy Object Renamed Report (Lepide Audit) Group Policy Object Modified Report (Lepide Audit)
	Report when new Active Directory user accounts are created, deleted, or modified.	Active Directory Object Created Report (Lepide Audit) Active Directory Object Deleted Report (Lepide Audit) Active Directory Object Modifications Report (Lepide Audit)
	Ensure we keep Active Directory clean of Inactive /Unwanted user accounts.	Active Directory Cleaner (Lepide Audit) Inactive Users Report (Lepide Audit)
Threat Detection	Identify incidents early on to prevent a breach of regulated data.	Any Threat Model Triggered (Lepide Detect) Users with Admin Privileges Report (Lepide Trust) Permissions by User Report (Lepide Trust)

		Inactive Users Report (Lepide Audit) Excessive Permissions Report (Lepide Trust) All Environment Changes Report (Lepide Audit) Anomaly Spotting (Lepide Detect) Files Copied Report (Lepide Audit) External Data Sharing Report (Lepide Audit) Potential Data Leakage Threat Model (Lepide Detect)
Access Governance	See when passwords or password policy changes were made.	Password Policy Modified Report (Lepide Audit) Password Age Policy Modified Report (Lepide Audit) Password Complexity Policy Modified Report (Lepide Audit) Password Encryption Policy Modified Report (Lepide Audit) Password History Policy Modified Report (Lepide Audit)
	Ensure we are storing personal data appropriately in line with our compliance requirements.	Data Classification (Lepide Identify) Classified Emails Report (Lepide Identify) Classified SharePoint Objects Report (Lepide Identify) Classified OneDrive Objects Report (Lepide Identify)

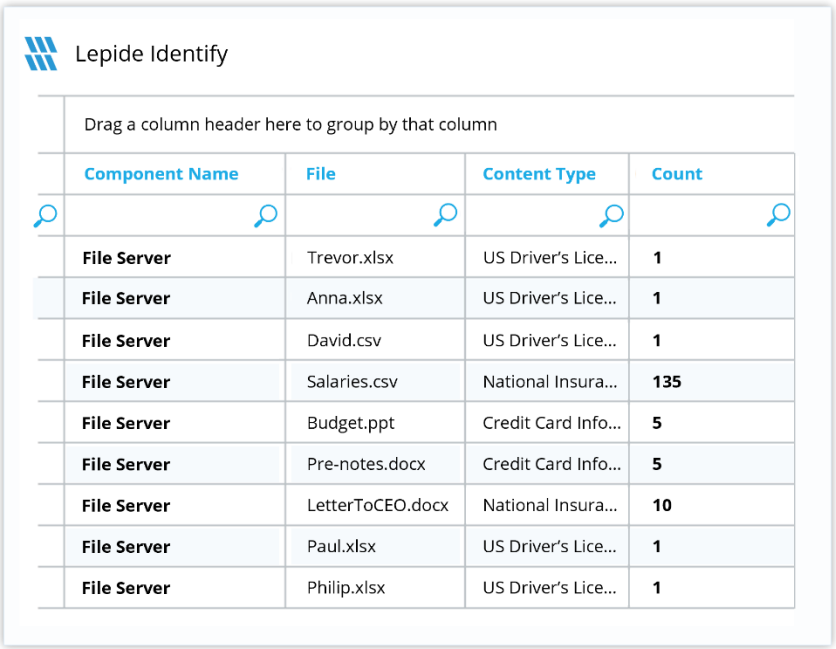
		Classified DropBox Objects Report (Lepide Identify) All Shares Report (Lepide Trust) Excessive Permissions by User Report (Lepide Trust) Excessive Permissions by Object Report (Lepide Trust) Permissions by User Report (Lepide Trust) Permissions by Object Report (Lepide Trust)
	See what personal or regulated data is being held and where is it being held.	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) All Shares Report (Lepide Trust) Excessive Permissions by User Report (Lepide Trust) Excessive Permissions by Object Report (Lepide Trust) Permissions by User Report (Lepide Trust) Permissions by Object Report (Lepide Trust)
	See what data we have inside the business that is subject to regulation.	Data Classification (Lepide Identify) Classified Files Report (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)

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:

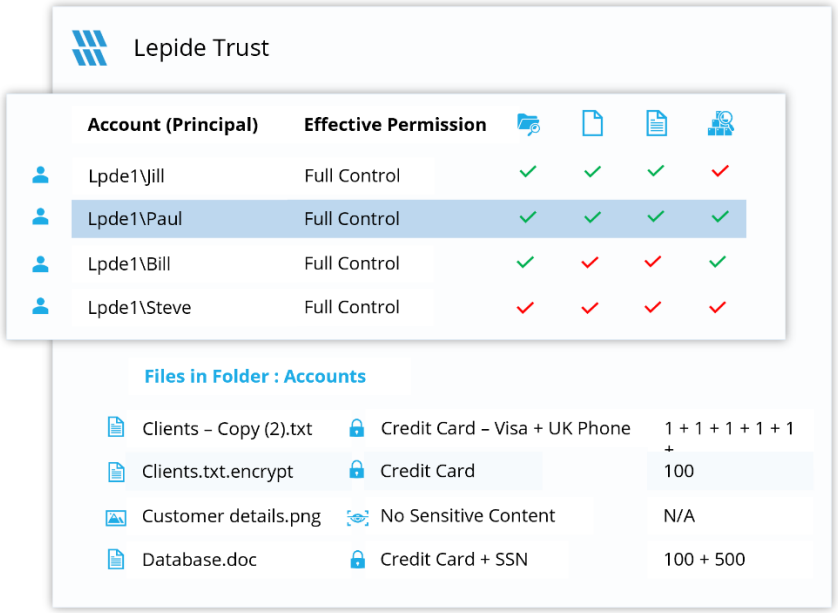
- Discover and classify data in real Tag data.
- Data valuation.
- Identify data most at risk.

For More Information:

https://www.lepide.com/data-security-platform/data-classification.html

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:

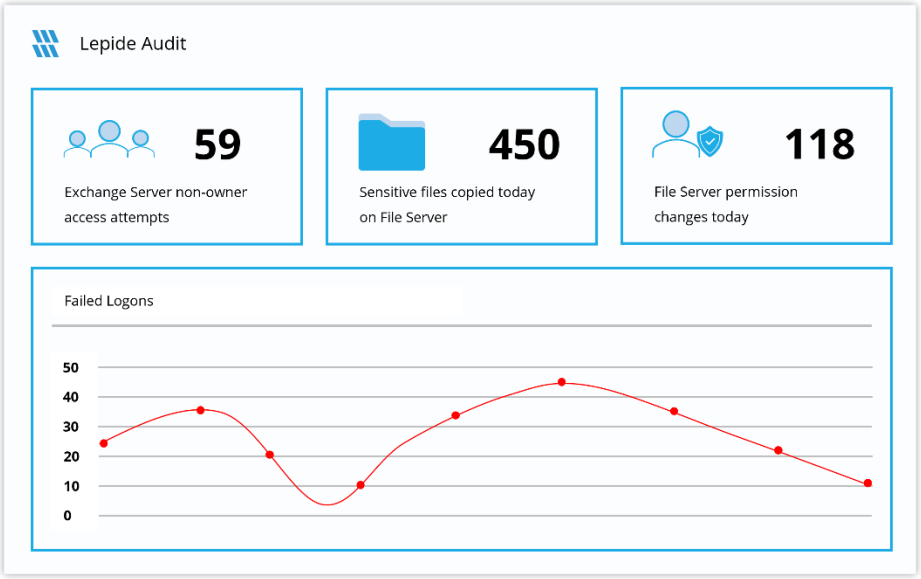
- Analyze permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

For More Information:

https://www.lepide.com/data-security-platform/permissions-and-privileges-analysis.html

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:

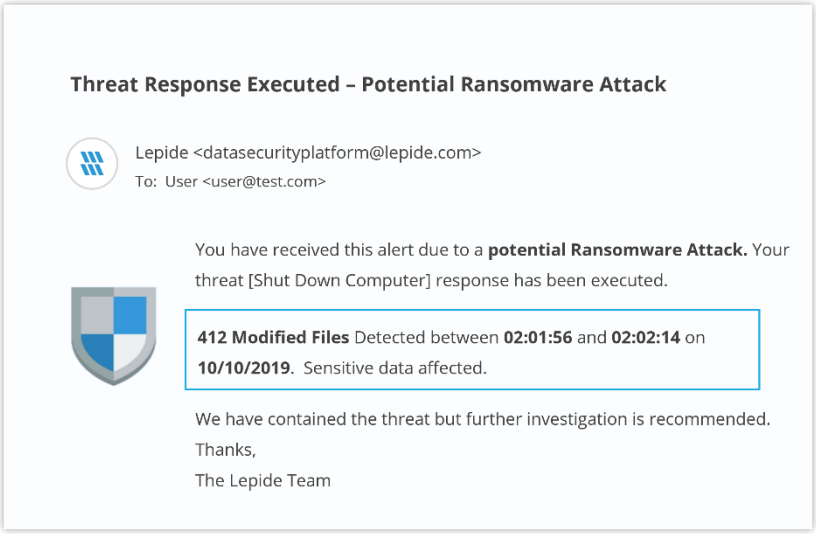
- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

For More Information:

https://www.lepide.com/data-security-platform/audit-and-report-changes.html

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/data-security-platform/react-to-data-security-threats-and-anomalies.html

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.