



ENABLEMENT GUIDE

ENABLING LEPIDE FOR

DATA LOSS

PREVENTION

Table of Contents

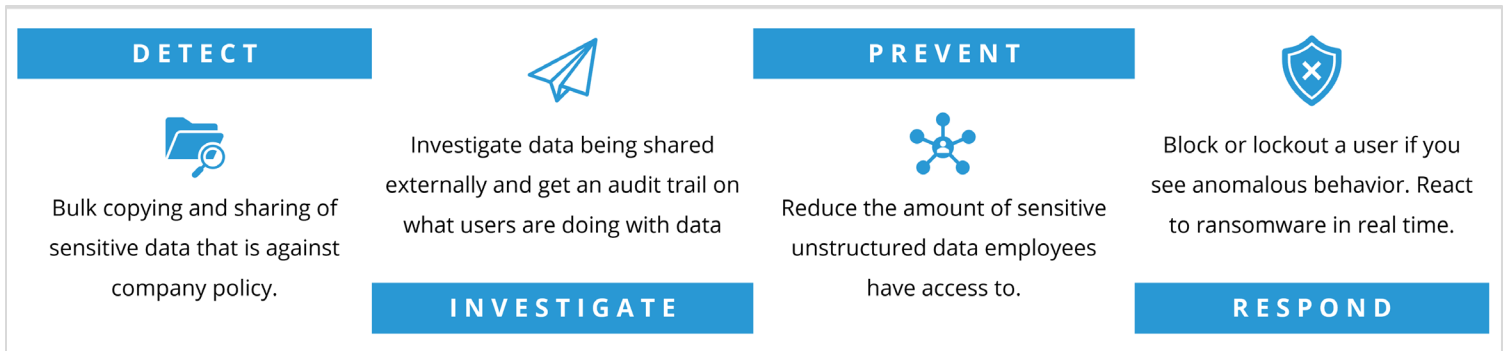
- 1. Introduction..... 3
- 2. Aligning Lepide for Data Loss Prevention..... 3
- 3. Lepide Core Capabilities 5
 - 3.1. - Lepide Identify 5
 - 3.2. - Lepide Trust 6
 - 3.3. - Lepide Audit 7
 - 3.4. - Lepide Detect 9
- 4. Support 10
- 5. Trademarks 10

1. Introduction

Data Loss Prevention is the means of being able to detect potential data breaches by monitoring, detecting, and in some cases, blocking sensitive data in motion and at rest. While we at Lepide cannot prevent the blocking of data leaving via USB or leaving via a web service on the endpoint, we can detect, alert and prevent sensitive data leaving via MS Teams, OneDrive, and MS Exchange. The level of knowledge we have in comparison to other DLP vendors when it comes to understanding both what data is sensitive, how the data is moving within the business and then across Exchange, Office 365 (Teams/OneDrive) makes our DLP proposition unique.

2. Aligning Lepide for Data Loss Prevention








There are a number of key questions that you need to be able to align Lepide for data loss prevention.



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

Category	Actions to Take	Technology to implement
Detect	Detect bulk copying of sensitive data.	<ul style="list-style-type: none"> File Copied Report (Lepide Audit) Mass Data Copy (FS) Threat Model (Lepide Detect) Mass Data Copy (FS) Threat Model Response – Disable User Account (Lepide Detect)
	Build alerts to be able to detect data being shared that is against company policy.	<ul style="list-style-type: none"> External Data Sharing Alert (Lepide Detect) Potential Data Loss Threat Model (Lepide Detect)


		<ul style="list-style-type: none">  Mass Data Copy Threat Model (Lepide Detect)  Files Copied Alert (Lepide Detect)
Investigate	See which sensitive or regulated data is being emailed internally or externally via MS Exchange	<ul style="list-style-type: none">  Potential Data Loss Threat Model (Lepide Detect)
	See what sensitive data is being shared externally via Teams or OneDrive.	<ul style="list-style-type: none">  Eternal Data Sharing in Office 365 Report (Lepide Audit)
	See what data is being copied inside the organization and who's doing it.	<ul style="list-style-type: none">  File Copied Report (Lepide Audit)  Mass Data Copy (FS) Threat Model (Lepide Detect)  All Modifications in File Server Report (Lepide Audit)
	Get a full audit trail of what a specific user is doing with sensitive data.	<ul style="list-style-type: none">  All Environment Changes Report (Lepide Audit)  All Modifications Reports – All Data Sources (Lepide Audit)
Prevent	How to reduce the amount of sensitive data my employees have access to reduce risk.	<ul style="list-style-type: none">  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 Trust)  Data Classification (Lepide Identify)

		<ul style="list-style-type: none">  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)
Response	Block or lockout a user if you see anomalous behavior.	<ul style="list-style-type: none">  Manually execute a threat response from the Lepide mobile app (Lepide Detect)  Create an Alert with an Automated Threat Response (Lepide Detect)
	Detect, and act on early stages of a ransomware attack to prevent data being leaked/breached.	<ul style="list-style-type: none">  Ransomware Threat Model (Detection and Response) (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.

 Lepide Identify

Drag a column header here to group by that column

Component Name	File	Content Type	Count
File Server	Trevor.xlsx	US Driver's Lice...	1
File Server	Anna.xlsx	US Driver's Lice...	1
File Server	David.csv	US Driver's Lice...	1
File Server	Salaries.csv	National Insura...	135
File Server	Budget.ppt	Credit Card Info...	5
File Server	Pre-notes.docx	Credit Card Info...	5
File Server	LetterToCEO.docx	National Insura...	10
File Server	Paul.xlsx	US Driver's Lice...	1
File Server	Philip.xlsx	US Driver's Lice...	1

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.

The screenshot displays the 'Lepide Trust' interface. It features a table of account permissions and a section for file sensitivity analysis.

Account (Principal)	Effective Permission	🔒	📄	📄	👤
Lpde1\Jill	Full Control	✓	✓	✓	✓
Lpde1\Paul	Full Control	✓	✓	✓	✓
Lpde1\Bill	Full Control	✓	✓	✓	✓
Lpde1\Steve	Full Control	✓	✓	✓	✓

Files in Folder : Accounts

File Name	Sensitivity Category	Score
Clients - Copy (2).txt	Credit Card - Visa + UK Phone	1 + 1 + 1 + 1 + 1
Clients.txt.encrypt	Credit Card	100
Customer details.png	No Sensitive Content	N/A
Database.doc	Credit Card + SSN	100 + 500

In Summary:

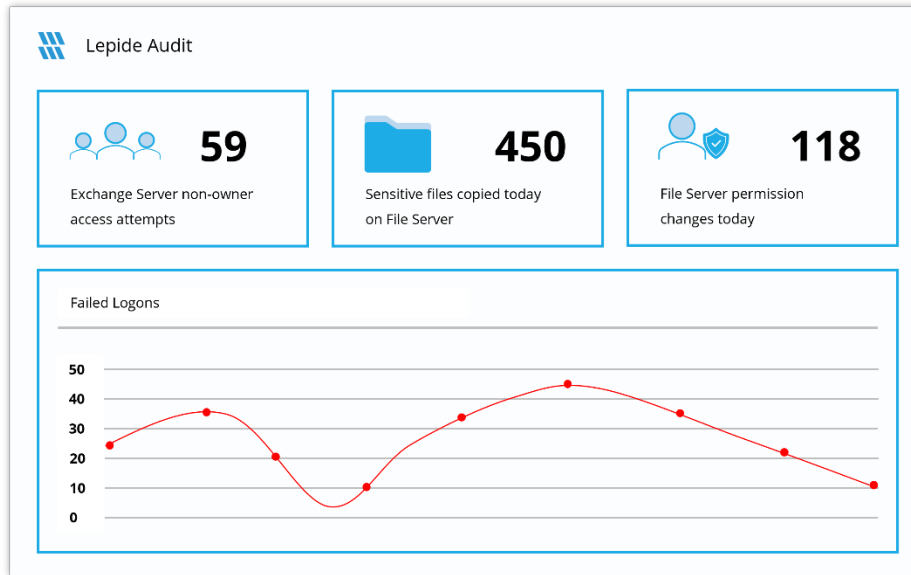
- Analyze permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

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.

Threat Response Executed – Potential Ransomware Attack

 Lepide <datasecurityplatform@lepid.com>
To: User <user@test.com>

You have received this alert due to a **potential Ransomware Attack**. Your threat [Shut Down Computer] response has been executed.

 **412 Modified Files** Detected between **02:01:56** and **02:02:14** on **10/10/2019**. Sensitive data affected.

We have contained the threat but further investigation is recommended.
Thanks,
The Lepide Team

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.