



ALIGNMENT GUIDE

ALIGNING LEPIDE FOR

RANSOMWARE

Table of Contents

- 1 Introduction..... 3
- 2 Aligning Lepide for Ransomware..... 3
- 3 Lepide Core Capabilities 6
 - 3.1 - Lepide Identify 6
 - 3.2 - Lepide Trust 7
 - 3.3 - Lepide Audit 8
 - 3.4 - Lepide Detect 9
- 4 Support 10
- 5 Trademarks 10

1 Introduction

Ransomware is arguably THE most pressing and potentially damaging security threat out there right now. Ransomware is where a company's data is encrypted, held at ransom, and released upon payment.

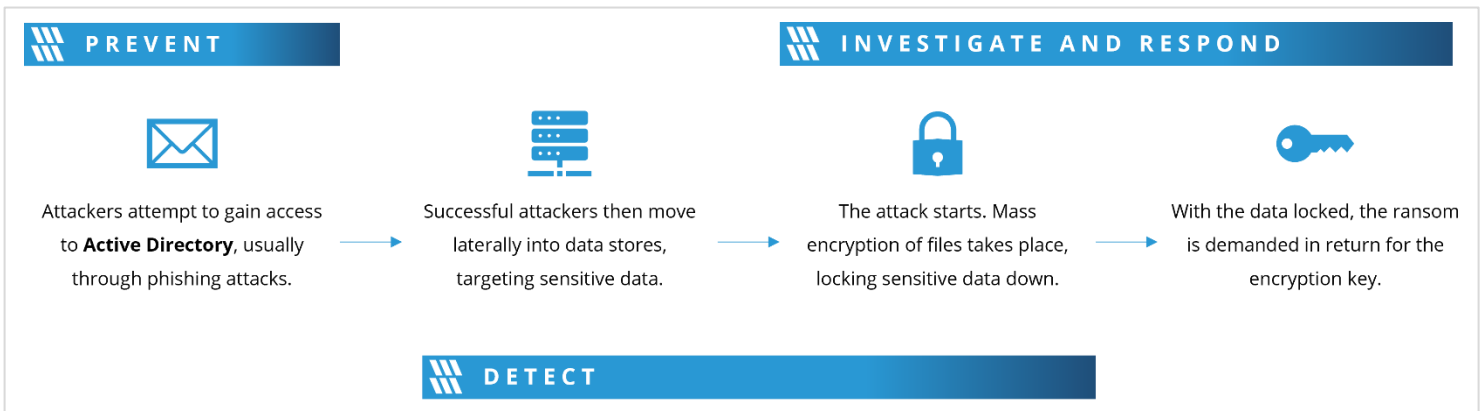
Ransomware often starts with a phishing email, leading to the compromise of an Active Directory account which is then used to spread across the corporate network. It will then attempt to elevate its access and permissions to access even more data to create the maximum amount of disruption.

In all cases, Ransomware relies on Active Directory as its means of moving across the network and in nearly all cases the data that is impacted by ransomware involves data stored on enterprise data stores such as a Windows File Server, OneDrive or SharePoint.


Due to our deep and unique knowledge of Active Directory and these enterprise data stores, using Lepide enables customers to have a significantly faster way to detect, respond and limit the damage of a ransomware attack.

2 Aligning Lepide for Ransomware








There are a number of key questions that you need to be able to answer to be able to detect, prevent, investigate and respond to ransomware attacks.



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

Category	Actions to Take	Technology to Implement
Detect	Detect changes in user behavior of a specific user account	 Anomaly Detection and Analysis (Lepide Detect)
	Detect 'en-mass' encryption events taking place across File Servers, OneDrive etc.	

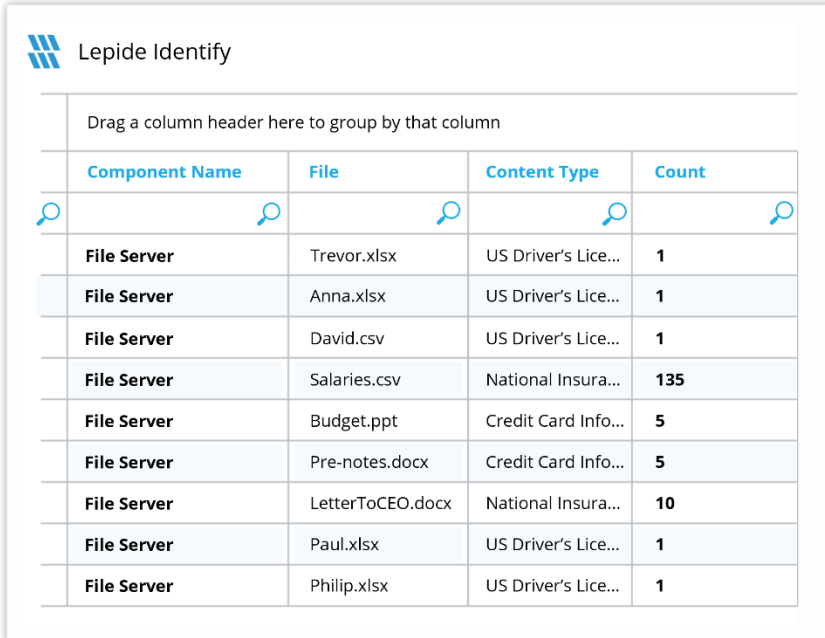
	<p>Detect permissions escalation of a specific user account</p> <p>Detect multiple instances of failed access attempts that look abnormal</p> <p>Detect user or group of users quickly trying to access large volumes of data</p>	<p>Potential Ransomware Attack Threat Model (Lepide Detect)</p> <p>Permissions Escalation (Groups) Threat Model (Lepide Detect)</p>
Prevent	Reduce your attack surface by limiting access to data based on only what is needed	<p>Inactive Users Report (Lepide Audit)</p> <p>Excessive Permissions by User Report (Lepide Trust)</p> <p>Permissions by User Report (Lepide Trust)</p> <p>Users with Admin Privileges Report (Lepide Trust)</p> <p>Open Shares (Lepide Trust)</p> <p>Data Classification (Lepide Identify)</p> <p>Increased Threat Surface Area Threat Model (Lepide Detect)</p>
Investigate	<p>Identify the potential source of the threat without having to rely on Windows event logs</p> <p>See what data could be affected by the threat based upon what the affected user has access to</p>	<p>All Modifications in File Server (Lepide Audit)</p> <p>Potential Ransomware Attack Threat Model (Lepide Detect)</p>

		<ul style="list-style-type: none"> Files Renamed (Lepide Audit) Read Failed (Lepide Audit) Permissions by User Report (Lepide Trust) Excessive Permissions by User (Lepide Trust)
Respond	<ul style="list-style-type: none">Automate the response when symptoms of a ransomware attack are detectedInstruct your SIEM or SOAR platform to engage based on these behaviorsRespond to a threat like this out of hours from your mobile device	<ul style="list-style-type: none"> Potential Ransomware Attack Threat Model with automated script (Lepide Detect) SIEM Integration (Lepide Detect) Set up an alert to mobile app with automated script (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.



The screenshot shows the 'Lepide Identify' interface. At the top left is the Lepide logo and the title 'Lepide Identify'. Below the title is a header row with the instruction 'Drag a column header here to group by that column'. The main table has four columns: 'Component Name', 'File', 'Content Type', and 'Count'. Each cell in the first row of the table has a magnifying glass icon. The table contains the following data:

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.

Lepide Trust

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

Files in Folder : Accounts

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:

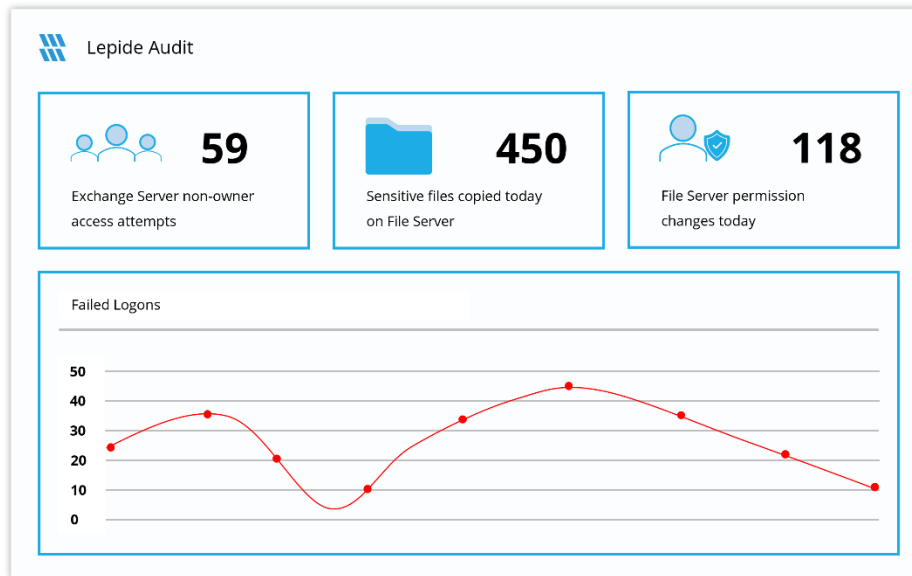
- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

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:

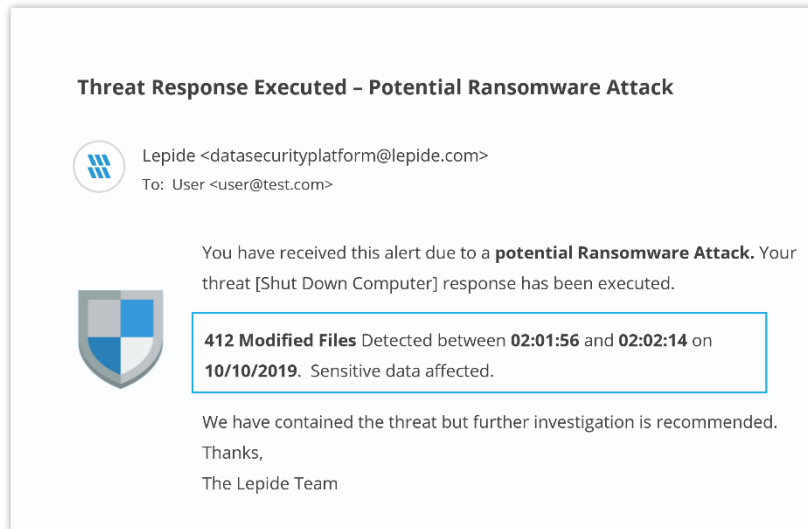
- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

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.