



ENABLEMENT GUIDE

ENABLING LEPIDE FOR

# REMOTE WORKERS

# Table of Contents

1. Introduction.....	3
2. Aligning Lepide for Remote Workers .....	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

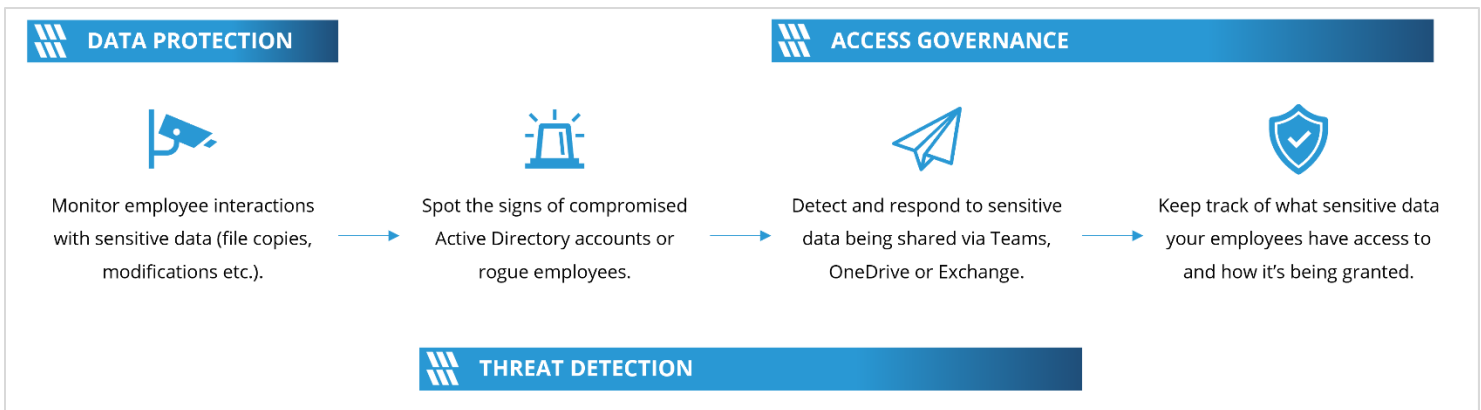
We can help organizations that are concerned about the security of their sensitive data posed by the additional risks posed by employees working from home. 73% of security teams believe that employees working from home pose a greater threat than those that are in the office. We can help alleviate some of these concerns.

We provide organizations with an audit trail to track every action every employee takes around their most sensitive data, along with real time alerts based on specific actions carried out around particularly sensitive files.

Using our anomaly detection or threat models we can identify behavior that could signify a rogue employee or a compromised user account. We also enable organizations to track the times/dates and trends around log on and log off activity and detect when there are trends and anomalies that look out of character that could signify a potential threat. We provide detailed audit trails of what sensitive data employees are sharing over MS Teams, OneDrive, SharePoint both internally and externally via Exchange.
















# 2. Aligning Lepide for Remote Workers







There are a number of key questions that you need to be able to answer to be able to protect your data, detect threats and comply with access governance.



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

Category	Actions to Take	Technology to implement
Data Protection	Monitor employees working with your [sensitive] data while working at home.	<ul style="list-style-type: none"> <li>Permissions by User Report (<a href="#">Lepide Trust</a>)</li> <li>Users with Admin Privileges Report (<a href="#">Lepide Trust</a>)</li> <li>Open Shares Report (<a href="#">Lepide Trust</a>)</li> </ul>

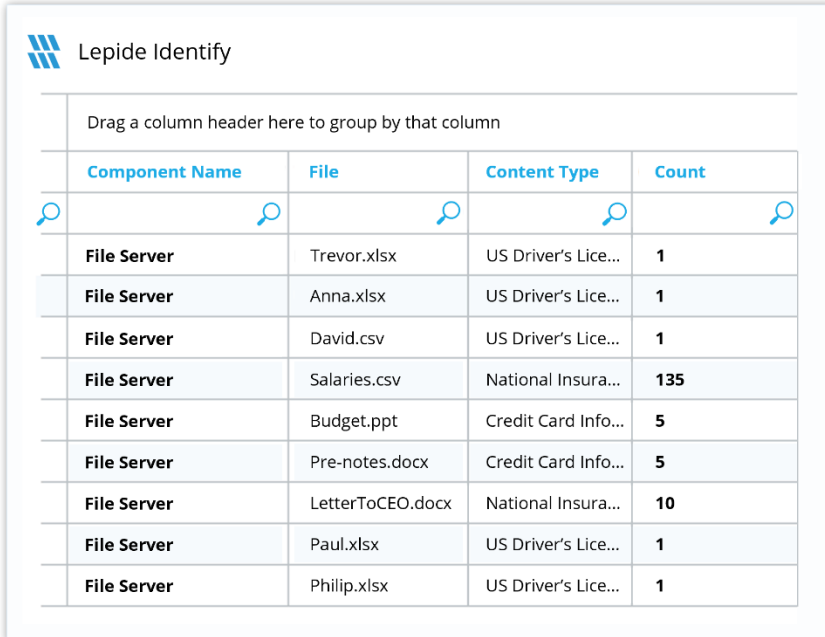
		<ul style="list-style-type: none"> <li> Data Classification (<a href="#">Lepide Identify</a>)</li> <li> File Server Modification Reports (<a href="#">Lepide Audit</a>)</li> <li> SharePoint Online Modification Reports (<a href="#">Lepide Audit</a>)</li> <li> OneDrive Modification Reports (<a href="#">Lepide Audit</a>)</li> <li> MS Teams Modification Reports (<a href="#">Lepide Audit</a>)</li> <li> External Data Sharing 0365 Report (<a href="#">Lepide Audit</a>)</li> <li> Mailbox Accessed by Non-owners Report (<a href="#">Lepide Audit</a>)</li> <li> Files Renamed Report (<a href="#">Lepide Audit</a>)</li> <li> Read Failed Report (<a href="#">Lepide Audit</a>)</li> <li> All Environment Changes Report (<a href="#">Lepide Audit</a>)</li> </ul>
	<p>Track the sensitive data your employees are copying. Ensuring that data does not sprawl.</p>	<ul style="list-style-type: none"> <li> File Copied Report (<a href="#">Lepide Audit</a>)</li> <li> Ransomware Threat Model (<a href="#">Lepide Detect</a>)</li> <li> SharePoint Online Document Copied Report (<a href="#">Lepide Audit</a>)</li> <li> Mass Data Copy Threat Model (<a href="#">Lepide Detect</a>)</li> </ul>
<p>Threat Detection</p>	<p>Spot when an employee's Active Directory accounts become compromised.</p>	<ul style="list-style-type: none"> <li> Brute force attack Threat Model (<a href="#">Lepide Detect</a>)</li> <li> Potential Password Compromise Threat Model (<a href="#">Lepide Detect</a>)</li> </ul>

		<ul style="list-style-type: none"> <li> Anomaly Spotting (<a href="#">Lepide Detect</a>)</li> <li> Active Directory Permissions Modifications Report (<a href="#">Lepide Audit</a>)</li> </ul>
	<p>Spot signs of an employee going rogue.</p>	<ul style="list-style-type: none"> <li> All Environment Changes Report (<a href="#">Lepide Identify</a>)</li> <li> Anomaly Spotting (<a href="#">Lepide Detect</a>)</li> <li> Threat Models (<a href="#">Lepide Detect</a>)</li> <li> Activity Outside of Business Hours Report (<a href="#">Lepide Audit</a>)</li> </ul>
	<p>Detect and respond to sensitive data being shared via OneDrive, MS Teams or Exchange.</p>	<ul style="list-style-type: none"> <li> External Data Sharing 0365 Report (<a href="#">Lepide Audit</a>)</li> <li> Create an Alert with an automated script (<a href="#">Lepide Detect</a>)</li> <li> Document Modification Reports (<a href="#">Lepide Audit</a>)</li> </ul>
<p>Access Governance</p>	<p>Keep track of what sensitive data your employees have access to.</p>	<ul style="list-style-type: none"> <li> Inactive Users Report (<a href="#">Lepide Audit</a>)</li> <li> Excessive Permissions by User Report (<a href="#">Lepide Trust</a>)</li> <li> Permissions by User Report (<a href="#">Lepide Trust</a>)</li> <li> Users with Admin Privileges Report (<a href="#">Lepide Trust</a>)</li> <li> Open Shares Report (<a href="#">Lepide Trust</a>)</li> <li> Data Classification Report (<a href="#">Lepide Identify</a>)</li> </ul>

## 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.

**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:

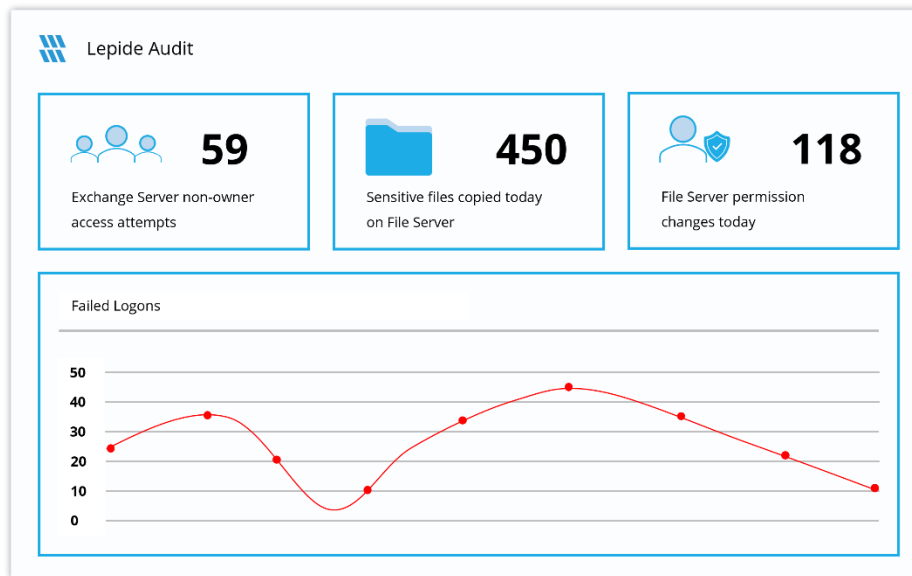
- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

### 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.

**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](mailto:sales@Lepide.com)

[support@Lepide.com](mailto: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.