



ALIGNMENT GUIDE

ALIGNING LEPIDE FOR

REMOTE WORKERS

Table of Contents

1.	Introduction.....	3
2.	Aligning Lepide for Remote Workers	3
3.	Lepide Core Capabilities	7
	3.1. - Lepide Identify	7
	3.2. - Lepide Trust	8
	3.3. - Lepide Audit	9
	3.4. - Lepide Detect	10
	3.5. - Lepide Protect.....	11
4.	Support	12
5.	Trademarks	12

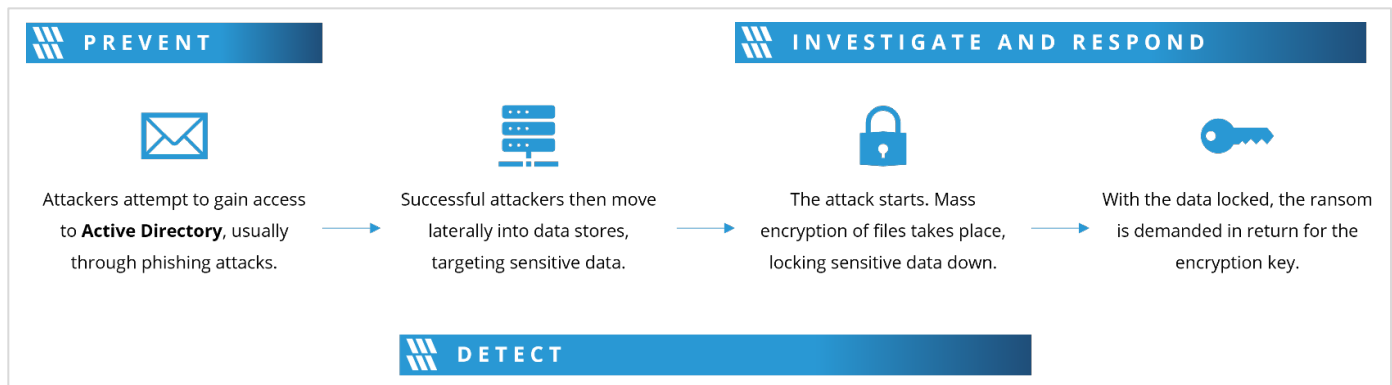
1. Introduction

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 their 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 can also provide detailed audit trails of what sensitive data employees are sharing over MS Teams, OneDrive, SharePoint both internally and externally via Exchange. Other security products simply do not have this depth of insight we have around Windows Technologies which is why we win.


















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 table below, we align Lepide technology to these questions:

Category	Actions to Take	Technology to implement
----------	-----------------	-------------------------

Data Protection	Employees working with our [sensitive] data while working at home.	<ul style="list-style-type: none">  Permissions by User Report (Lepide Trust)  Users with Admin Privileges Report (Lepide Trust)  Open Shares Report (Lepide Trust)  Data Classification (Lepide Identify)  File Server Modification Reports (Lepide Audit)  SharePoint Online Modification Reports (Lepide Audit)  OneDrive Modification Reports (Lepide Audit)  MS Teams Modification Reports (Lepide Audit)  External Data Sharing 0365 Report (Lepide Audit)  Mailbox Accessed by Non-owners Report (Lepide Audit)  Files Renamed Report (Lepide Audit)  Read Failed Report (Lepide Audit)  All Environment Changes Report (Lepide Audit)
	Sensitive data our employees are copying. Ensuring that data does not sprawl.	<ul style="list-style-type: none">  File Copied Report (Lepide Audit)  Ransomware Threat Model (Lepide Detect)  SharePoint Online Document Copied Report (Lepide Audit)  Mass Data Copy Threat Model (Lepide Detect)

Threat Detection	An employee's Active Directory accounts becoming compromised.	 Brute force attack Threat Model (Lepide Detect)  Potential Password Compromise Threat Model (Lepide Detect)  Anomaly Spotting (Lepide Detect)  Active Directory Permissions Modifications Report (Lepide Audit)
	Spotting signs of an employee going rogue.	 All Environment Changes Report (Lepide Identify)  Anomaly Spotting (Lepide Detect)  Threat Models (Lepide Detect)  Activity Outside of Business Hours Report (Lepide Audit)
	Detecting and responding to sensitive data being shared via OneDrive, MS Teams or Exchange.	 External Data Sharing 0365 Report (Lepide Audit)  Create an Alert with an automated script (Lepide Detect)  Document Modification Reports (Lepide Audit)
Access Governance	Keeping track of what sensitive data our employees have access to. How we can reduce risk.	 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 Report (Lepide Identify)

		 Permissions Remediation (Lepide Protect)
--	--	---

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 / Lepide Auditor / Reports / File Server / Classified Files

[Generate Report](#) [Export](#)

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

Total Reports : 50

First Previous 1 / 1 Next Last

50 / page

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.

[illegible]

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

Oct 1, 2024 - Oct 1, 2024

Generate Report Export

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

First Previous 1 / 898 Next Last

10 / Page

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 / Lepide Auditor / Reports / Active Directory / Failed Logon

Mar 26, 2024 - Mar 26, 2024 Generate Report Export

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

First Previous 1 / 1 Next Last

50 / page

In Summary:

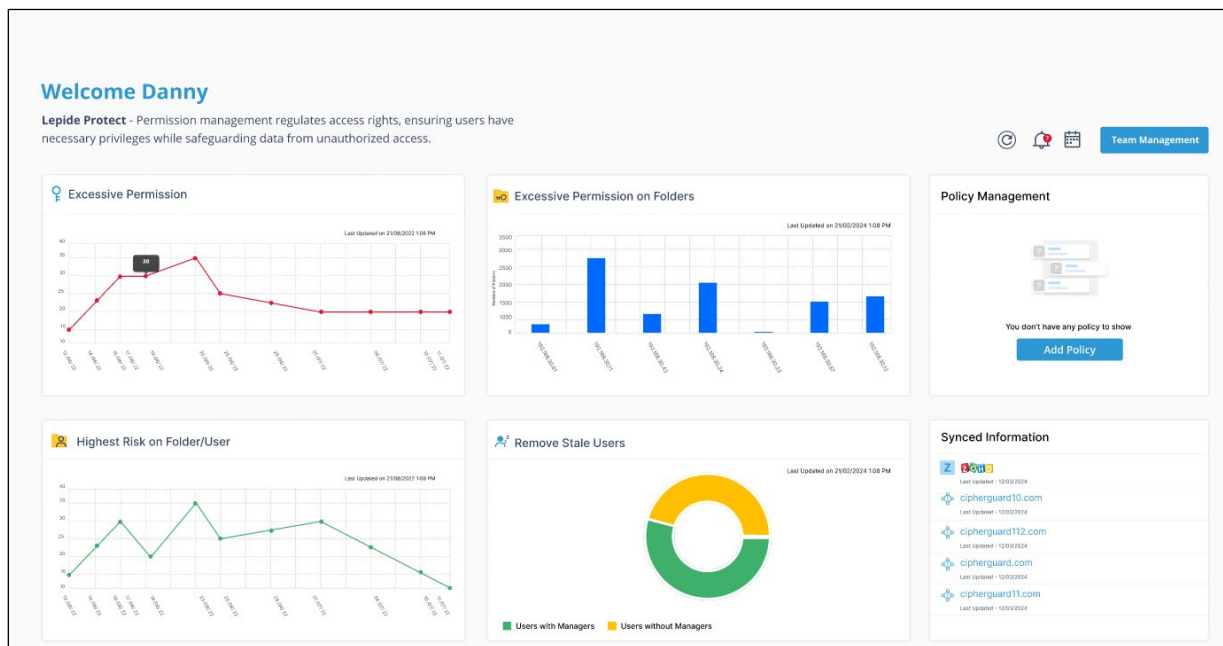
- Detect threats in real time with pre-defined threat models.
- Baseline/profile employee behavior.
- Identify anomalous employee behavior.
- Alert and respond to threats in real time.

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.



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.

