Lepide

Aligning Lepide for Generative AI.

Use case guide.

Contents

1 Executive Summary

1.1 Generative AI and Data Security Risk

Generative AI technologies, such as Microsoft Copilot and other large language models (LLMs), are transforming how organizations access and interact with data. By enabling users to query and generate insights from vast volumes of information instantly, these tools significantly increase productivity—but also introduce a new class of data security risks as AI will only be as secure as your data permissions.

Generative AI does not create new data exposure risks; rather, it amplifies existing weaknesses in data access, permissions, and governance. Over-permissioned users, unclassified sensitive data, and poor access controls can result in confidential information being unintentionally surfaced through simple natural language prompts. This makes previously hidden or hard-to-find data instantly discoverable, increasing the risk of data leakage, insider threats, and compliance violations.

1.2 Why Lepide is Critical for Safe AI Adoption

To safely adopt generative AI, organizations must first ensure that their data environment is secure, well-governed, and properly controlled. The Lepide Data Security Platform enables organizations to achieve this by providing complete visibility and control over sensitive data across on-premises and cloud environments.

Lepide helps organizations:

- **Identify and classify sensitive data** before it is indexed or exposed to AI tools
- **Eliminate excessive permissions** to ensure only authorized users can access critical data
- **Continuously audit user and data activity** across Active Directory, Microsoft 365, and file systems
- **Detect anomalous behavior and potential threats** in real time using machine learning and threat models
- **Automate remediation and enforce least-privilege access** to reduce the overall attack surface

By addressing these foundational security gaps, Lepide ensures that generative AI tools only surface data that users are explicitly authorized to access.

1.3 Aligning Lepide to the Generative AI Lifecycle

Lepide supports organizations across the full generative AI lifecycle:

- Pre-Deployment (Data Readiness):

  Discover, classify, and secure sensitive data while remediating excessive permissions to prevent overexposure.

- Post-Deployment (Monitoring and Control):

  Continuously monitor user activity, detect abnormal behavior, and respond to threats to ensure AI-driven access remains secure and compliant.

1.4 Business Outcomes

By aligning Lepide with generative AI initiatives, organizations can:

- **Prevent AI-driven data leakage** by securing access before deployment
- **Enable safe and compliant use of AI tools** such as Microsoft Copilot
- **Reduce insider and external threat risks** amplified by AI-powered data discovery
- **Maintain continuous visibility and auditability** of how sensitive data is accessed and used
- **Strengthen Zero Trust and data governance frameworks** in an AI-enabled environment

Generative AI has the potential to unlock significant business value—but only if deployed on a secure data foundation. Without proper controls, it can quickly become a force multiplier for data exposure and security risk as AI will only be as secure as your data permissions.

Lepide ensures that organizations can embrace generative AI with confidence by delivering the visibility, control, and intelligence needed to protect sensitive data—before, during, and after AI adoption.

2 What is Generative AI

Generative AI is artificial intelligence (AI) that can create original content, for example, text, images or video, in answer to a user's request. It relies on sophisticated machine learning models that simulate the learning and decision-making processes of the human brain. These models work by identifying and encoding patterns and relationships within vast amounts of training data and then use that information to understand the natural language requests of users and return relevant new content. It is important to note that Generative AI does not create new data risk, it exposes existing weaknesses in data access, permissions, and governance at scale.

3 Generative AI Risk Scenarios

Generative AI tools such as Microsoft Copilot transform how users access data by removing the need to search manually. Instead, users can retrieve and summarize information instantly using natural language prompts.

While this improves productivity, it also introduces new risks. If data is overexposed, unclassified, or poorly governed, AI will surface it—quickly and at scale.

Below are common real-world scenarios that highlight how generative AI can unintentionally expose sensitive data:

1. Overexposed Data via Simple Prompts

A user asks: *"Show me all employee salary data"*

If permissions are too broad, AI can instantly surface sensitive HR or payroll information that the user should not have access to.

- **Risk**: Unauthorized access to confidential data due to excessive permissions
- **Impact**: Data privacy breaches, regulatory violations, and reputational damage

2. Sensitive Data Discovered Due to Lack of Classification

A user asks: *"Summarize our latest financial reports"*

If sensitive files are not properly classified or labeled, AI may include confidential or restricted information in its response.

- **Risk**: Exposure of regulated or business-critical data
- **Impact**: Compliance failures and unintended disclosure of sensitive information

3. AI Amplifying Insider Threats

A malicious or careless employee uses AI to query: *"Show me all documents related to mergers and acquisitions"*

AI accelerates their ability to locate and access high-value data across multiple systems in seconds.

- **Risk**: Rapid data discovery and aggregation by insider threats
- **Impact**: Increased likelihood of data theft or misuse

4. Compromised Accounts Leveraging AI

An attacker gains access to a user account and uses AI to explore: *"What sensitive files can I access?"*

AI helps the attacker quickly identify valuable data without needing deep system knowledge.

- **Risk**: Accelerated lateral movement and data discovery during a breach
- **Impact**: Faster and more severe data exfiltration

5. Unintentional Data Leakage Through AI Responses

A user asks AI to generate a report or summary, which includes sensitive information pulled from multiple sources.

The user then shares this output externally without realizing it contains confidential data.

- **Risk**: Indirect data leakage through AI-generated content

- **Impact**: Loss of intellectual property or exposure of regulated data

6. Data Sprawl Increasing AI Exposure

Sensitive data stored across file shares, cloud platforms, and collaboration tools is not centrally governed. AI aggregates and surfaces this data regardless of where it resides.

- **Risk**: Widespread exposure due to uncontrolled data sprawl
- **Impact**: Increased attack surface and difficulty maintaining compliance

In Summary

- Generative AI dramatically lowers the barrier to accessing data.
- Users no longer need to know where data is stored as AI finds it for them.
- Without proper data classification, access controls, and continuous monitoring, generative AI can quickly become a force multiplier for data exposure.
- Lepide helps organizations mitigate these risks by ensuring that only the right data is accessible - before and after AI deployment.

To mitigate these risks, organizations must ensure that sensitive data is controlled, permissions are tightly managed, and all access is continuously monitored both before and after AI deployment.

4 Aligning Lepide for Generative AI

AI makes everything searchable instantly. But by implementing Lepide, you can ensure that only the right data is searchable.

Lepide can be used to identify sensitive data on file servers, fix excessive permissions, continuously audit AD/Entra ID and file changes, and alert on risky sharing or group modifications before they are indexed by Copilot.

Without Lepide, AI becomes a data breach accelerator.

The phases of Generative AI involve the lifecycle of building, deploying, and maintaining a generative AI system and so there are several factors to consider for Pre and Post Deployment of Generative AI which are explained as follows:

4.1 Pre Deployment – Harden Directories and Prepare Data Stores

Before deploying generative AI tools such as Microsoft Copilot, organizations must ensure their data environment is **secure, well-governed, and properly controlled**.

Generative AI will index and surface data based on existing permissions and access structures. If those permissions are too broad, or sensitive data is unclassified, AI can instantly expose information that was previously difficult to find.

AI doesn't create risk—it reveals it at scale.

This makes pre-deployment the most critical phase for reducing data exposure.

Lepide helps organizations establish a secure foundation by ensuring that only the right data is accessible—before AI is introduced.

In summary, pre-deployment is about getting your data under control before AI amplifies its risks.

If sensitive data is unclassified or overexposed, generative AI will make it instantly accessible.

AI will only be as secure as your data permissions.

Lepide ensures that before AI is deployed, your data is secure, access is controlled, and risk is minimized.

Category	Actions to Take	Technology to implement	Outcome
Data Protection	Eliminate Excessive Permissions and Enforce Least Privilege. Reduce data sprawl	Inactive Users Report (Lepide Audit) User Permission Analysis and Visibility Reporting (Lepide Trust) Object Permission Analysis and Visibility Reporting (Lepide Trust) Open Shares Report (Lepide Audit) Data Classification Reporting (Lepide Identify) Increased Threat Surface Area Threat Model (Lepide Detect) Permissions Escalation Threat	Reduces insider threat and accidental data exposure.

		Models (Lepide Detect) Permissions Remediation (Lepide Protect)	
	Clean Up Active Directory and Remove Risky Accounts	Inactive Users Report (Lepide Audit) Active Directory Cleaner (Lepide Audit) Remove Inactive Users (Lepide Protect)	Minimizes attack surface and reduces inactive account risk
	Get an audit report of what employees are doing with regulated data.	Data Classification Reporting (Lepide Identify) All Environment Changes Report (Lepide Audit) All Data Interaction Reports for File Server, SharePoint, SharePoint Online, OneDrive (Lepide Audit) All Mailbox Access Reports (Lepide Audit)	Prevents sensitive data from being exposed through AI queries Improves accountability and data handling transparency Ensures safe Copilot deployment
	See who has privileged access to Active Directory.	Users with Admin Privileges Report (Lepide Trust) Active Directory Permissions Reports (Lepide Trust)	Reduces risk of privilege abuse Supports enforcement of least privilege and role-based access control

Access Governance	Ensure we are storing personal data appropriately in line with our compliance requirements.	Data Classification Reporting (Lepide Identify) All Shares Report (Lepide Trust) User Permissions Reporting (Lepide Trust) Object Permissions Reporting (Lepide Trust)	Reduces exposure of personal or sensitive data in non compliant storage Improves data mapping and accountability
	See what personal or regulated data is being held and where it is being held.	Data Classification Reporting (Lepide Identify) All Shares Report (Lepide Trust) User Permission Analysis and Visibility Reporting (Lepide Trust) Object Permission Analysis and Visibility Reporting (Lepide Trust)	Provides full data discovery for compliance audits Prevents AI-driven data leakage
	See what data we have inside our business that is subject to regulation.	Data Classification Reporting (Lepide Identify)	Enhances regulatory readiness and data governance posture Ensures classification and labeling of sensitive data Supports compliance reporting and policy enforcement

4.2 Post Deployment - Monitor, Prove, and Continuously Tighten

Once generative AI tools such as Microsoft Copilot are deployed, the challenge shifts from preparation to **continuous control**. At this stage, organizations must ensure that AI-driven access to data remains secure, compliant, and aligned with business policies.

Generative AI introduces a new dynamic:
data is no longer accessed through traditional search—it is surfaced instantly through prompts.
This means organizations must monitor not just user activity, but **what AI is accessing, surfacing, and exposing on behalf of users.**

Lepide provides the visibility and control needed to govern this new access layer.

In summary, with post-deployment, the focus is no longer just on securing data—it's on **governing how AI interacts with that data**.

AI will only be as secure as your data permissions.
Lepide ensures that as AI surfaces information at scale, it only exposes what users are authorized to see and nothing more.

Category	Actions to Take	Technology to implement	Outcome
Data Protection	Control access as users change roles (joiners, movers, and leavers) to maintain appropriate access.	User Permission Analysis and Visibility Reporting (Lepide Trust) Inactive Users Report (Lepide Audit) Permissions Remediation (Lepide Protect)	Prevents privilege creep and unauthorized retention of access Strengthens zero-trust enforcement
	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)	Ensures traceability of all changes for audit and compliance review Enables rapid incident investigation and rollback

			Reduces risk of unauthorized account access permissions
	Keep track of changes to group memberships and group policies.	Group Policy Object Changes Reporting (Lepide Audit)	Maintains security integrity of group policies Prevents privilege escalation through group changes
	Report when new Active Directory user accounts are created, deleted, or modified.	Active Directory Change Auditing and Visibility Reporting (Lepide Audit)	Reduces exposure from unauthorized account creation Improves readiness for security audits and compliance reviews
	Review all Copilot usage reports	Copilot Access Reporting (Lepide Trust) Copilot Usage Comparison Report (Lepide Audit) All Copilot Searches Report (Lepide Trust) Data Accessed by Copilot Report (Lepide Audit) Sensitivity Label Changes Report (Lepide Audit)	Enables AI adoption with compliance confidence Spot unexpected spikes by team, location, or data store Reduces risk of sensitive data exposure via prompts Monitor all data, including sensitive data, accessed by Copilot Prevents AI-driven data leakage

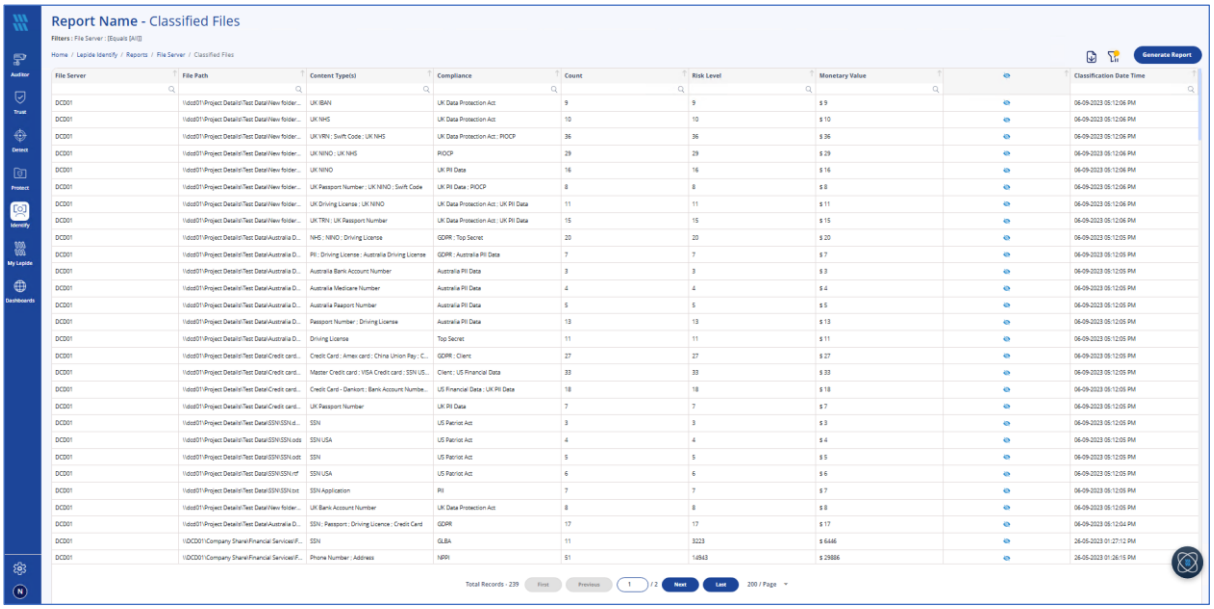
Threat Detection	Identify incidents early on to prevent a breach of regulated data.	Any Threat Model Triggered (Lepide Detect) User Permission Analysis and Visibility Reporting (Lepide Trust) Inactive Users Report (Lepide Audit) Anomaly Spotting (Lepide Detect) External Data Sharing Report (Lepide Audit)	Enables proactive detection of anomalous user behavior Helps demonstrate continuous monitoring controls
Access Governance	See when passwords or password policy changes were made.	Password Policy Changes Reporting (Lepide Audit)	Detects unauthorized changes to password settings Strengthens authentication and policy enforcement controls
Detect	Detect changes in user behavior of a specific user account	Anomaly Detection and Analysis (Lepide Detect)	Early identification of abnormal activity (eg, sudden access spikes or changes in behavior) to prevent ransomware from spreading.
	Detect 'en-mass' encryption events taking place across File Servers, OneDrive etc.		Immediate alerts for mass file encryption or renaming, allowing quick isolation of compromised systems.
	Detect permissions escalation of a specific user account	Potential Ransomware Attack Threat Model (Lepide Detect)	Detection of unauthorized privilege escalation attempts to

		Permissions Escalation (Groups) Threat Model (Lepide Detect)	stop lateral movement before impact
	Detect multiple instances of failed access attempts that look abnormal		Identification of brute-force or credential stuffing attempts, helping to block compromised accounts early.
	Detect user or group of users quickly trying to access large volumes of data		Alerts triggered for data exfiltration or encryption-like behaviors to enable rapid containment.

5 Lepide Core Capabilities

5.1 - 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:

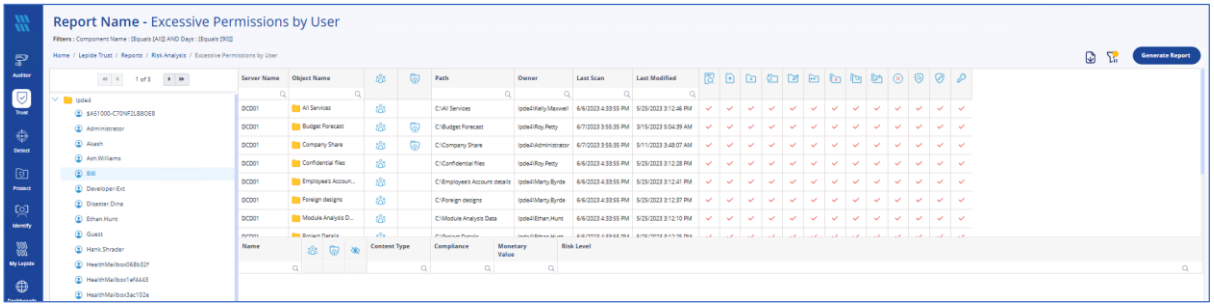
- Discover and classify data in real Tag data.
- Data valuation.
- Identify data most at risk.

For More Information:

https://www.lepide.com/lepide-identify/

5.2 - 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:

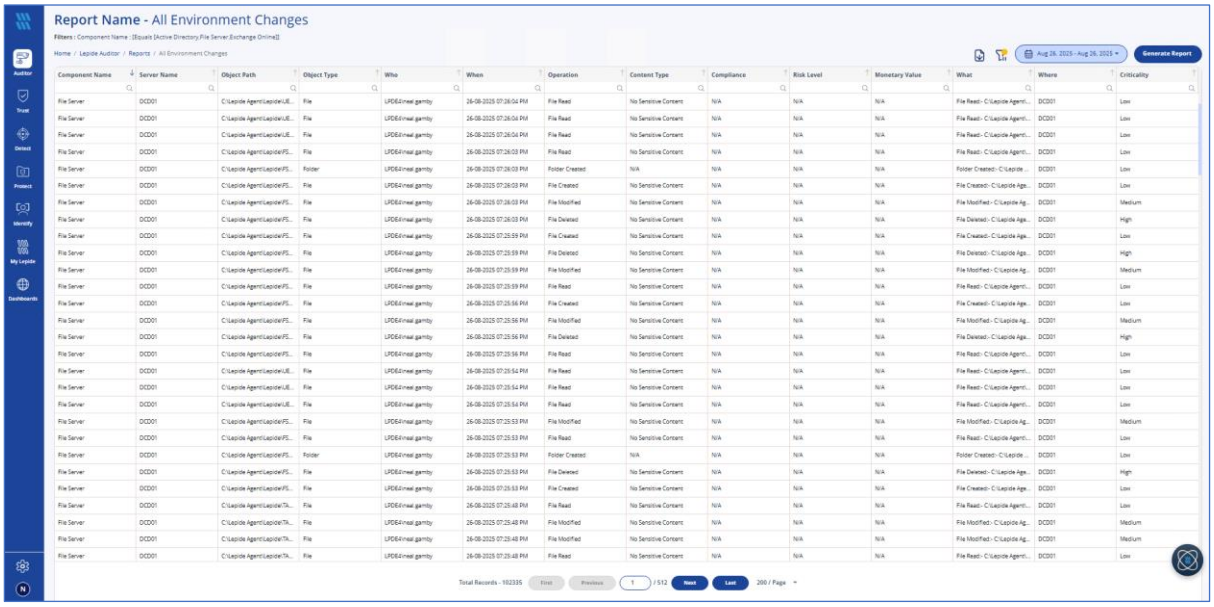
- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

For More Information:

https://www.lepide.com/lepide-trust/

5.3 - 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:

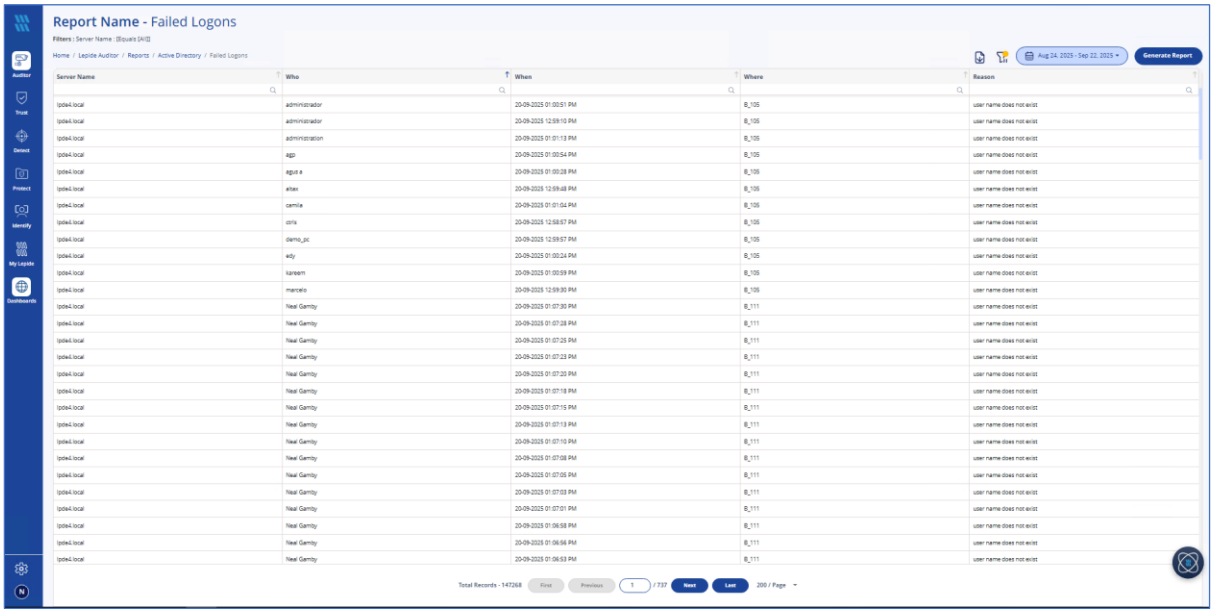
- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

For More Information:

https://www.lepide.com/lepideauditor/

5.4 - 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:

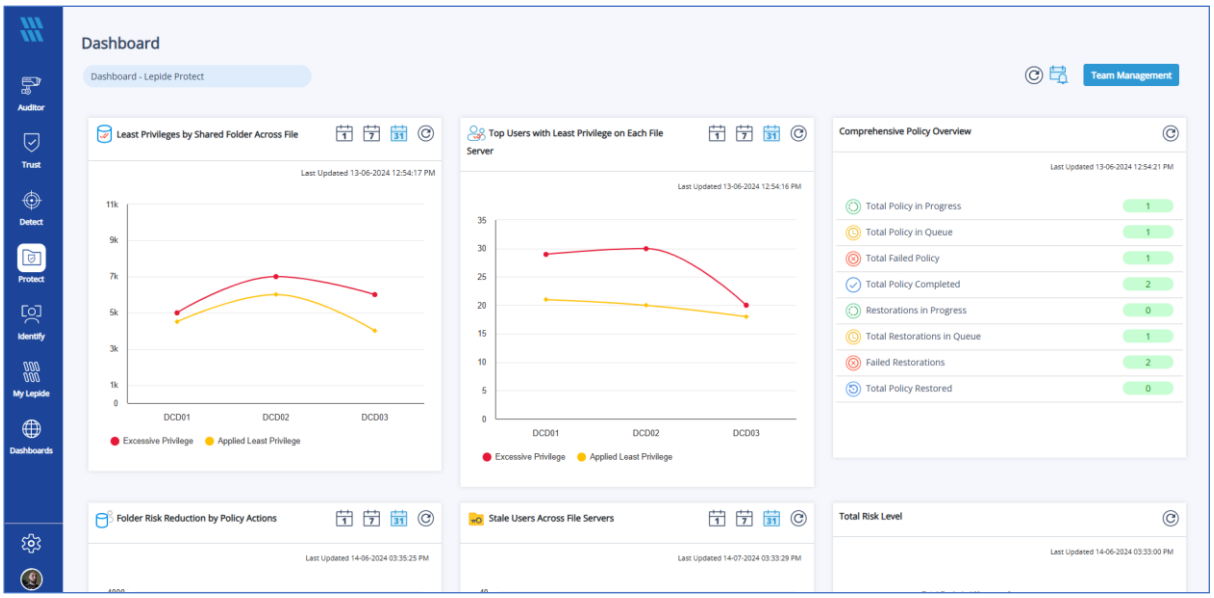
- Detect threats in real time with pre-defined threat models.
- Baseline/profile employee behavior.
- Identify anomalous employee behavior.
- Alert and respond to threats in real time.

For More Information:

https://www.lepide.com/lepide-detect/

5.5 - 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/

6 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/.

7 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.