Lepide

Lepide Data Security Platform

An Overview

On-Premise Auditing

Active Directory Auditor

Audit changes to AD, including before & after values, with the ability to rollback changes and recover objects.

Group Policy Auditor

Track and rollback all changes to Group Policy objects as well as the policies within, including local policies, password policies.

Exchange Server Auditor

Audit changes to Exchange objects and attributes in AD, the configuration, security, and use of Exchange, as well as mailbox access.

SQL Server Auditor

Monitor and report on all logins, administrative changes, and client use of SQL Server instances.

SharePoint Server

Audit all use and changes to farms, servers, sites, storage, security, and content.

Active Directory Cleaner

Automatically clean-up inactive user and computer accounts - disable, delete, reset password, or move them to another OU.

User Password Expiration Reminder

Get periodic password expiry reminders, know about 'soon to expire', 'never expire' and ‘expired passwords’ data in any domain.

File Server Auditor

We believe all organizations should instantly be able to see 'who, what, where and when' files and folders are created, accessed, modified, copied or deleted at the click of a button. We also think it's essential that organizations are easily able to track and compare permissions across their data. Lepide's File Server auditing solution addresses the challenges of the rise of the insider-threat and the reporting requirements associated with common regulatory compliance mandates. We give IT teams the power to see more, faster. Track access attempts and changes to your files and folders with granular who, what, when and where information. Understand when your users are copying your files to help maintain security and integrity of data. Real time alerts, threshold alerts and pre-defined reports for all security and compliance needs.

Data Classification

DDC for File Server

Discover where sensitive data is for files and folders, classify your sensitive data, tag your sensitive data, group into certain categories, automatically score your data with a risk value to highlight area of potential risk.

Available for:

- File Server
- Exchange Server (Online and On-Prem)
- SharePoint Server (Online and On-Prem)
- OneDrive

Session Monitoring

Invisible User Monitoring. The solution will not be visible to the user during the monitoring process, so you can be confident that your employees will be entirely unaware of its installation or execution. Lepide will automatically start monitoring activities the moment systems are started and will continue to monitor even if a user restarts the system. Session recording can also take place offline, allowing you to access recordings at your convenience. Through the solution, you can re-start, turn off or completely shut down a computer on which you have seen unauthorized or unwanted activity taking place. Warning messages can be sent to the user in question before any further action is taken. You also have the option to periodically display custom pop-up message on all monitored computers. Delegate Viewing Rights to Specific Users. The viewing aspect of the monitoring feature can be installed on any system you wish. The administrator can delegate monitoring rights for all computers or specific computers only to any specified user. You can also search for and download any video recordings for future reference.

Office 365

Amazon S3 Auditing

Audit Amazon S3 Buckets to determine who's accessing data within the buckets, and who is making configuration changes.

Azure AD Auditor

Track's configuration changes, monitor privileged users/groups and provides a full audit trial of every user authentication.

Dropbox Auditing

Track changes to file and folders, insight into Dropbox link sharing, monitor permissions to critical data.

Exchange Server Auditor Online

Audit changes to Exchange objects and attributes in AD, the configuration, security, and use of Exchange, as well as mailbox access.

OneDrive for Business

Track file and folder level changes, track security groups and configuration changes.

SharePoint Server Online

Audit all use and changes to farms, servers, sites, storage, security, and content.

Skype for Business

Shows users.

MS Teams

Monitor User Activities in Microsoft Teams. The collaboration that MS Teams provides creates unique security challenges that many solutions cannot cope with. Lepide enables you to get real visibility over how your users are engaging with Teams and when sensitive data is being shared, to help you respond to threats and prevent breaches.

G Suite

Understanding the logon activity of business users is critical in getting better insight into how and when your organizations employees are gaining access to your core systems and data. We also help you keep track of failed logins to G Suite to better understand if there could be a potential security risk or someone is trying to gain access with invalid credentials.

Track Changes Made to Sensitive Data:

If you are providing access to your companies most sensitive data through Google Drive, then it's important to understand who interacting with that data. Through creations, deletions, modifications and altering access via permission changes, we help by giving you better insight across your shared data.

Track Administrative Changes in G Suite:

Just as its important to understand how your business users are interacting with the data and the surrounding applications with G Suite, you should easily be able to identify how and when users are being given access. Administrators or privileged users hold all the keys to the applications, Lepide can help you keep account of all administrative activities from privilege escalation to system configuration change ensuring the applications and data are available only to the people who actually need access.