Lepide

Datasheet

Lepide for **AZURE ACTIVE DIRECTORY**

Summary

Monitor Azure AD Changes

Delivers essential audit information about changes being made to Azure AD with who, what, where and when information.

Track Azure AD Logons

Spot when a large number of failed logons are occurring which could indicate a brute force attack.

Better Azure AD Reporting

View Azure AD changes through detailed, pre-defined reports that can be scheduled to deliver automatically.

Audit Permission Changes

Get insight into Azure AD permission changes to help maintain a policy of least privilege.

Find What You Need

Build advanced search filters to investigate and interrogate your audit data on a more granular level.

Key Security Features for Active Directory

Lepide Azure AD Auditor helps you to audit changes made to Azure AD configurations, permissions, user profiles and much more through a combination of pre-defined audit reports.

Granular Monitoring of Azure AD Changes

Lepide Azure AD Auditor enables you to monitor and audit all changes made in Azure AD to ensure the appropriate change processes are being followed. Ensure complete accountability through visibility is available to catch any unauthorized changes or changes that may have an impact on access to other critical applications, systems or data within your business. Our Azure AD auditor tracks who made what changes, where they were made and when; including user or group creation, modification and deletion, failed and successful login attempts, password changes, resets and much more.

Detailed Azure AD Audit Reports

Tracking Azure Active Directory changes using Lepide could not be simpler. Our Azure AD auditing solution continuously tracks and monitors critical changes with regards to user accounts, passwords, logins and more. This information is collected, formatted and presented in easy-to-read Azure AD audit reports that can be scheduled for regular delivery or accessed any time on-demand.

Customized/Interactive Search

Easily build advanced search filters to interrogate your Azure AD data more quickly. All of your searches can then be saved to the console to enable quick access. Our Azure AD auditing solution enables you to search based on component/server name, object path/type, the criticality of the change and much more. This kind of interactive/customizable searching and filtering will help you increase the speed with which you are able to investigate changes to your Azure AD environment.

Overcome the Limitations of Native Azure Auditing

Our Azure AD audit reports allow you to get more context from changes than you would be able to get from native audit logs. With information presented in a readable and useful way, you can speed up your incident investigation and detect and react quicker to unwanted changes. Microsoft only allows you to store logs for 90 days, which seriously limits your ability to investigate historic incidents or access old log information. Our Azure AD Audit solution stores your audit trail for years, enabling you to overcome many of the limitations of native Azure AD auditing.

What We Audit in Azure Active Directory

Auditing Azure AD Configuration Changes

Lepide Azure AD Auditor provides you with granular audit detail on every aspect of the configuration changes made in your Azure AD environment. The solution proactively and continuously audits and monitors on configuration changes to give you real insight into your Azure AD environment. Get in-depth information and visibility into changes to object modifications, service principals, applications, user roles, policies and more.

Azure AD Permissions Auditing

Using Lepide Azure AD Auditor will ensure you get the insight you need into whenever permissions are being changed. In order to maintain a secure IT environment, we recommend you operate on a policy of least privilege (where users have the minimum levels of permissions possible). Lepide Azure AD Auditor enables you to maintain such a policy by helping to detect whenever your Azure AD permissions change.

Audit Successful and Failed Azure AD Login Attempts

As an IT administrator, it's important to know whenever users are logging on to Azure AD. If you spot a large number of failed logons over a short period of time, for example, this could be indicative of an attempted hack. Lepide Azure AD Auditor enables you to generate information on both successful and failed logon events.

Privileged Azure AD User/Group Monitoring

Understanding how and when users are being added to the privileged security groups in Azure AD is a vital part of maintaining a secure IT environment. Our Azure AD audit solution allows you to keep track of activities performed by your privileged users and groups. You can use this information to help you enforce a policy of least privilege where users only have access to the data and applications they need to do their job effectively.