Lepide

Datasheet

Lepide for

ACTIVE DIRECTORY

Summary

Analyze Risks to AD

Identify where your weaknesses are through high-level dashboards so that you can address potential vulnerabilities.

More Than Just Visibility

Combine auditing with machine learning, user behavior and more to detect and react to threats faster.

Monitor Your Attack Paths

Attackers often exploit AD credentials as their entry paths. Monitor logons, changes and user behavior to prevent attacks.

Simplify Access Rights

Easily answer questions about who has privileged access and how they got it so that you can better visualize your domain.

Improved Investigations

Investigate security incidents faster and with more accuracy with real time alerts and a simple, unified audit trail.

Compliance Readiness

Pre-defined reports for common security and compliance concerns, including PCI, HIPAA, GDPR, CCPA, SOX, and more.

Key Security Features for Active Directory

Deploying an Active Directory auditing solution, like Lepide Active Directory Auditor, can help you monitor, detect and alert on suspicious or unwanted Active Directory changes. Through a combination of real-time monitoring, pre-defined reports and powerful alerting capabilities, Lepide Active Directory Auditor enables you to get better visibility into Active Directory changes. Here are just some ways in which our Active Directory Auditor can help your business.

Monitor Changes with an Intuitive Dashboard

Lepide Active Directory Auditor offers a 360º Radar Tab, that allows you to monitor your whole Active Directory environment changes. Instantly see a summary of the total number of changes per administrator, per source and even by trend to help you identify change/event anomalies. Our Live Feed feature enables you to monitor all changes being made in real time to ensure that you are constantly aware of what's happening in your critical IT.

Granular Audit Reports

We offer a single log for a single change displaying who, what, where and when the changes are made. We then provide this data to you through more than 100 relevant reports to help you address all manner of compliance, security, and IT operations challenges. Each report can be further customized with advanced filtration, searching, sorting, and other auditing functions. These Active Directory audit reports can also be shared with other users through a secure web console.

Real Time Alerts

Lepide AD Auditor has two types of alerting mechanisms – one is real-time alerting, which alerts on critical changes in real-time, and the other is threshold-based alerts, where you can define the threshold limit for every change. Real time alerts allow you to identify threats immediately and trigger automated responses to shut down threats before they manifest in breaches.

Security and Compliance Reports

Our Active Directory auditing software has dedicated predefined reports to meet the IT-related regulations for numerous compliances, including PCI, SOX, GLBA, HIPAA, FISMA, CCPA and GDPR. Generate reports that show how your Active Directory environment is adhering to the selected compliance in just a few clicks. Inbuilt, predefined, and customized reports allow you to meet other compliance requirements not listed here.

Track Logon Activity and Spot Anomalies

Strange logon/logoff activity, such as users logging on out of office hours, or multiple failed logons in a short space of time, can be the signs of a potential threat. Getting logon/logoff details for all users from the Event Viewer is like looking for a needle in a haystack. Our solution simplifies this search with simple yet detailed Active Directory audit reports on failed logon events, concurrent logon sessions, and users logged on to multiple computers. Our solution also sends real-time and threshold-based alerts for successful user logon or logoff and can spot anomalies in logon/logoff behavior.

Rollback Unwanted Changes

From time to time, a user account may be modified in error or a Junior Administrator may accidentally delete an OU. Our rollback feature enables you to reverse changes made in a single click. It restores everything to exactly as it was before the change – including group memberships, attributes, permissions and more.

What We Audit in Active Directory

Permission Changes

Whenever permissions change, you need to be aware of it. Our Active Directory auditing solution keeps track of every permission change in the Active Directory, records it in its granular reports, and sends real-time or threshold-based alerts for such critical changes. It also allows you to view all permissions to an object and compare the permissions of an object between two dates. All effective permissions held by an Active Directory Object are also displayed. You can also conduct historical permission analysis between two specific time intervals. You can easily reverse the unwanted permission changes to an ideal state (that you have defined and captured earlier).

Security Settings

Lepide Active Directory Auditor offers you dedicated reports to help keep track of the security settings of Active Directory objects. In addition to permissions, you can also compare audit settings, and ownership of an object between intervals. You have the option to track all changes made in audit settings and object ownership, and also view them on any particular date.

Our solution lets you search for an object in the audit entries or see a list of owners of a selected object.

Privileged User Monitoring

Lepide Active Directory Auditor lets you track the members of administrative groups in Active Directory to give you a clear picture of the privileged users. Our solution also offers a way to track all activities of Active Directory privileged users and sends real-time or threshold-based alerts for any critical change made by a privileged user account.

Troubleshoot Account Lockouts

In any IT environment, it is advised that you lock accounts that are inactive for a long period of time or on which suspicious activities were taking place. However, locking an Active Directory user account can impact other activities linked to that account, which could be a mess left to the IT team to clean up. Lepide Active Directory Auditor comes helps you better handle user account lockouts, by auditing the account lockouts and providing the option to unlock or reset their passwords. You can also investigate which tasks, services, or processes will be impacted because of this account lockout.

Active Directory Objects' State Reports

Lepide Active Directory Auditor periodically captures backup snapshots of Active Directory objects and saves their state. You can use these snapshots to generate historical reports on the state of users, groups, computers, and organizational units (the four important objects)

at any given point in time. It gives you a clear picture of exactly when any of these objects were created or modified and what it's properties are.