Lepide

Datasheet

Data Security Platform

Benefits

The Lepide Data Security Platform offers a simple, yet powerful way of detecting insider threats, preventing data breaches and meeting compliance regulations. Data discovery and classification, user and entity behavior analytics, anomaly spotting and change auditing enable you to get complete visibility into the security of your sensitive data.

Data Protection

Find out which of your data is most at risk today and take the required steps to reduce that risk.

Compliance

Get the visibility and reports you need to meet compliance audits, including HIPAA, PCI, SOX, GDPR, CCPA and more.

Detect/React to Threats

Reduce the time it takes to detect and respond to threats through increased visibility and automation.

Solution

The Lepide Data Security Platform combines all the security solutions provided by Lepide into a single, powerful platform.

Lepide Auditor

Audit, report and alert on all changes being made to security states, data and permissions. Spot changes that leave you in a vulnerable state, generate compliance ready reports and get a complete audit trail for changes.

Lepide Data Access Governance

Analyze access rights across key platforms in your environment to spot users with excessive permissions.

Lepide User Behavior Analytics

Analyze critical changes to data that your users are making and spot anomalies that could affect your security posture. Report on file copy events, modifications, deletions and much more.

Lepide Data Classification

Find out where you most sensitive data resides and why it is sensitive through our discovery and classification functionality. Whether your data is stored in the cloud or on-premise, you can categorize it based on risk and relation to various compliance mandates.

Key Features

Intuitive Dashboard

Instantly see a summary of all changes made from a single intuitive dashboard. Identify any potential issues with server performance. Instantly see changes as they are happening with our Live Feed feature.

Granular Reporting

Hundreds of compliance ready reports for easy and quick access to compliance-related data. Quickly identify the 'who, what, where and when' of any change.

Real Time Alerting

Create instant alerts when specified events occur. Build threshold alerts to help you identify anomalies. Receive real time alert straight to the app, console or a specific email address.

Mobile App

Live Feed of changes as they happen. Designed to work on any Apple or Android enabled device. Enables you to track changes on the go.

Data Access Governance

Discover and classify your most sensitive data in relation to security and compliance concerns. Get detailed analysis and alerts on user behavior through a simple integration. Ensure appropriate access rights by analyzing permissions to your unstructured data.

Universal Auditing

Lepide Data Security Platform can now audit any cloud platform with out of the box templates and an easy to use interface.

Basic System Requirements

- Dual Core Processor or higher
- Recommend RAM - 8 GB
- Required Disk Size - Minimum 30 GB
- Any of the following Windows OS (both 32-bit and 64-bit platforms):
  Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows Server 2008 / Windows server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016

Supported Servers

- Active Directory plus Group Policy Objects
- Exchange Server
- Office 365
  - Exchange Online
  - SharePoint Online
  - Azure Active Directory
  - OneDrive
  - Skype for Business
- SharePoint Server
- SQL Server
- Windows File Server (both 32-bit and 64-bit versions)
- NetApp Filer
- Dropbox for Business
- Amazon S3
- G Suite
- Any other cloud platform through universal auditing integration

Prerequisites

NET Framework 4.0 or later

Any of the following SQL Server versions:
SQL Server 2008 / SQL Server 2008 R2 / SQL Server 2012 / SQL Server 2014 / SQL Server 2016 / SQL Server 2008 Express / SQL Server 2008 R2 Express / SQL Server 2012 Express / SQL Server 2014 Express

For Auditing Active Directory
Event Viewer of all domain controllers, including primary domain controller, should be accessible.

For Auditing Group Policy Objects
For Agent-based auditing, Windows PowerShell 2.0 should be installed on server.
.NET Framework 4.0 should be installed both on server to be monitored and computer where solution is installed.
GPMC should be installed on the computer where solution is installed.
For Agentless Group Policy Auditing
The solution should be installed on client machine.
Windows PowerShell 2.0 for client machine.

For Non-owner Mailbox Access Auditing
Exchange Server 2010 / Exchange Server 2013 / Exchange Server 2016

For Auditing Exchange Online
NET Framework 4.0 or later / Windows PowerShell 3.0 or later

For Auditing SharePoint Server
Connectivity and accessibility to the instance of SQL Server, which is interlinked with SharePoint Server
Microsoft System CLR Types for SQL Server 2012, Microsoft SQL Server 2012 Management Objects, .NET Framework 4.0, and Microsoft Visual C++ 2010 x64 Redistributable Setup should be installed the server to be monitored.
.NET Framework 4.0 on the computer where solution is installed.

For Auditing SQL Server
The selected SQL Server should be in the same forest network.
The computer, on which solution is installed, should be a member of the domain instead of a workgroup.

For Auditing NetApp Filer
The agent to audit NetApp Filer can only be installed on any client system, but it requires GPMC.MSC (Group Policy Management Console) for installation.
If you need permission changes on files and folders in NetApp Filer, then it is recommended to use synchronous mode to connect to NetApp Filer

For Health Monitoring
WMI Services should be up and running