

# Security That Starts With Data

## Discovery & Classification

*Where is your sensitive data?*

## Permissions & Privileges

*Who has access to what?*

## User & Entity Behavior

*How are users interacting with data?*

## States & Changes

*Does your environment pose a risk?*

# LepideAuditor

LepideAuditor offers a simple, cost effective and scalable means of auditing and monitoring changes made to **Active Directory, Group Policy, File Server, Exchange, SQL, SharePoint, Dropbox, Amazon S3, G Suite and Office 365**. It also allows organisations to keep track of file and folder level access, modifications and permission changes. With hundreds of predefined reports and a real time alerting capabilities, LepideAuditor can effectively address all manner of security, operations and compliance challenges.

### Intuitive Dashboard

- ✓ Instantly see a summary of all changes made from a single portal
- ✓ Identify any potential issues with server performance
- ✓ Instantly see changes as they are happening with our LiveFeed feature.

### Granular Reporting

- ✓ Pick from hundreds of pre-set reports to help with compliance, security and operations
- ✓ Quickly identify the 'who, what, where and when' of any change
- ✓ Delegate Reports to specified users via a secure, web-based console

### 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

### Data Access Governance

- ✓ Discover, classify, score and tag your most sensitive data with File Server Resource Manager
- ✓ Get detailed analysis and alerts on user behaviour through a simple integration
- ✓ Ensure appropriate access rights by analyzing permissions to your unstructured data

### Roll Back Changes

- ✓ Single click roll back of changes made to Active Directory Objects and Group Policy Object
- ✓ Leaves everything exactly as it was before the change
- ✓ Restores deleted Active Directory objects even if not available in tombstone, "logically deleted state", or Active Directory Recycle Bin

### Mobile App

- ✓ LiveFeed of changes as they happen
- ✓ Designed to work on any Apple or Android enabled device
- ✓ Enables you to track changes on the go

### Session Monitoring

- ✓ Monitor users invisibly and automatically
- ✓ No limitations on the number of computers and systems that can be monitored
- ✓ Take action by locking or restarting computers, logging off users or by sending warning messages

### SIEM Integration

- ✓ Integrate with any SIEM solution, including Splunk, LogRhythm, IBM QRadar, HP ArcSight and more
- ✓ Send specific events to your SIEM through LepideAuditor
- ✓ Get context to the raw audit data and speed up detection and response

"LepideAuditor provided us with complete visibility over what was happening in our IT environment in a simple, scalable and cost-effective way."



## 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 for Auditing

### Active Directory plus Group Policy Objects:

- Windows Server 2008 / Windows server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016

### Exchange Server:

- Exchange Server 2007 / Exchange Server 2010 / Exchange Server 2013 / Exchange Server 2016

### Office 365

- Exchange Online
- SharePoint Online
- Azure Active Directory
- OneDrive
- Skype for Business

### SharePoint Server:

- SharePoint Server 2010 / SharePoint Foundation 2010 / SharePoint Server 2013 / SharePoint Foundation 2013 / SharePoint Server 2016

### SQL Server:

- SQL Server 2008 / SQL Server 2008 R2 / SQL Server 2012 / SQL Server 2014 / SQL Server 2016

### Windows File Server (both 32-bit and 64-bit versions):

- Windows Server 2003 / Windows Server 2003 R2 / Windows Server 2008 / Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016

### NetApp Filer:

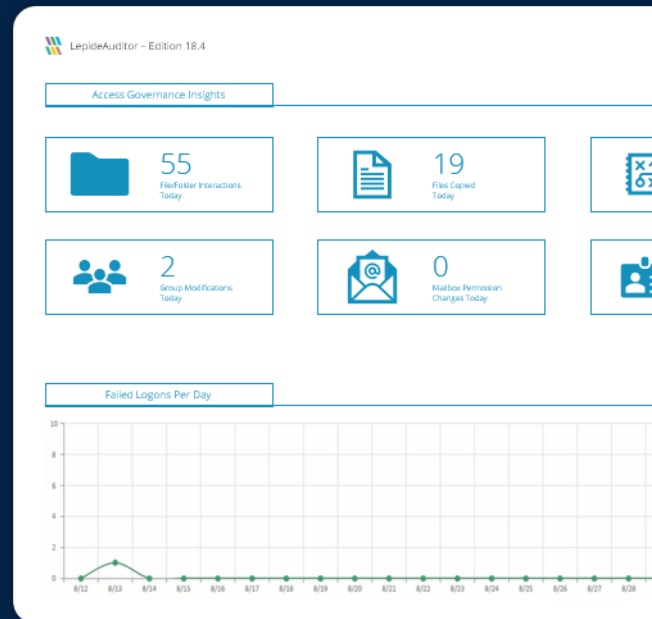
- NetApp 7-Mode Configuration
  - Successfully audits and report events for NetApp Filer Data ONTAP 7.2 or later.
  - Complete Feature Availability for ONTAP 7.3.4 or later.
- Cluster Mode 8.3 or later

### Cloud Components:

- Dropbox for Business
- Amazon S3
- G Suite

## 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



## Product Experts



USA/Canada: +1-800-814-0578  
UK/Europe: +44 (0)208 099 5403



sales@lepide.com

## Technical Gurus



USA/Canada: +1-800-814-0578  
UK/Europe: +44 (0)208 099 5403



support@lepide.com