Lepide

Datasheet

Data Access Governance

Data Access Governance Solution

With Lepide, you have a complete solution that enables you to identify where your sensitive data is, get detailed analysis and alerts on user behavior and ensure access rights by analyzing permissions to your unstructured data and reversing unwanted changes.

Classify Sensitive Data

Determine where your sensitive data is and why it is sensitive. Tag, classify and score that data based on the content.

Prevent Unauthorized Access

Find out who has access to your data and how it was granted, and reverse excessive permissions from within the solution.

Monitor User Behavior

Find out what your users are doing with your data and whether the changes they are making are affecting your security.

Detect Anomalies

Get instant notifications when users are making changes they have never made before, including single point anomalies.

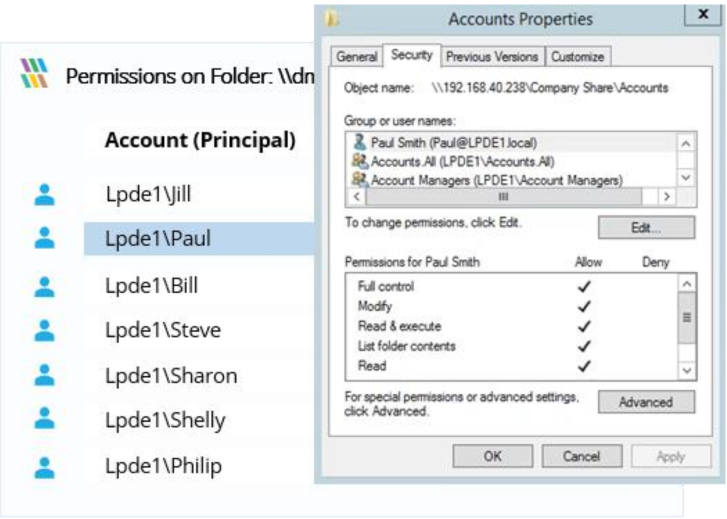
Detailed Pre-Set Reports and Real Time Alerts

Hundreds of pre-set reports related specifically to security and data access governance challenges and real time alerts for changes being made.

Spot and Remediate Excessive Permissions

When permission changes are made that could lead to unauthorized or unnecessary access to sensitive data, your potential attack surface and risk of data breaches increases. With Lepide, you can spot these permission changes and reverse the change from within the solution itself.

Lepide also automatically detects users with excessive permissions to help you speed up and streamline remediation.



Permissions on Folder: \\dn

Account (Principal)
Lpde1\Jill
Lpde1\Paul
Lpde1\Bill
Lpde1\Steve
Lpde1\Sharon
Lpde1\Shelly
Lpde1\Philip

Accounts Properties

Object name: \\192.168.40.238\Company Share\Accounts

Group or user names:

Paul Smith (Paul@LPDE1.local)
Accounts.All (LPDE1\Accounts.All)
Account Managers (LPDE1\Account Managers)

To change permissions, click Edit.

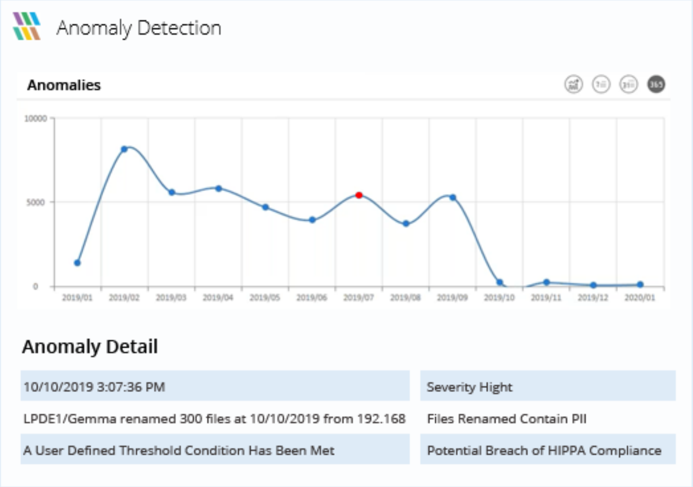
Permissions for Paul Smith	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	

For special permissions or advanced settings, click Advanced.

Get Visibility Over Anomalous User Behavior

.

With our intelligent anomaly spotting you can detect and react to user behavior that may be putting you at risk of security breaches. Lepide can detect single point anomalies and enables you to action automated threat response templates to help shut down threats before they cause irreparable damage.



Anomaly Detection

Anomalies

Anomaly Detail

10/10/2019 3:07:36 PM	Severity Hight
LPDE1/Gemma renamed 300 files at 10/10/2019 from 192.168	Files Renamed Contain PII
A User Defined Threshold Condition Has Been Met	Potential Breach of HIPPA Compliance

How Else Does Lepide Help?

View All Your Most Sensitive Files and Folders in a Single, Flexible Report

A single report displays all your sensitive files and folders and allows you to filter, search or group for easy interrogation of the data. This feature of Lepide Data Security Platform enables you to add context to the raw data Microsoft provides and helps satisfy compliance audits. The data collected from multiple storage locations is then consolidated and centrally stored for multilocation reporting capabilities.

Spot Potential Data Breaches Involving Your Sensitive Data

With just a simple right click, you can instantly create alerts to track critical changes to a sensitive file or folder. Our threshold-based alerting allows you to create alerts if a group of conditions are met. You can apply contextual filters, so you only receive alerts around your most sensitive files. Get instant notifications when files are copied, moved, deleted, modified and renamed – or if permissions are modified. Alert when sensitive files are accessed, or access attempts have been made over a period of time.

Run One of Our Pre-Set User Behavior Reports or Build Your Own

With multiple predefined reports and intuitive report builders around you unstructured data, we’re able to schedule a report with multiple filters and a range of reporting options based upon either one, a few of or all the files that contain sensitive data. These reports can be scheduled to be automatically delivered to a user of your choice via email; enabling you to automate the delivery of the report to either the data owner, your DPO, a compliance officer or Information Security Manager. Reports have been specifically designed for security and compliance mandates such as PCI, GDPR, SOX, HIPAA and more.

Group Your Sensitive Data Easily by Type, Location, Data Owner and Last Accessed Date

With our flexible reporting platform, you’re able to drag, drop and group reports by either classification type (i.e. Credit Card, PII) by data owner, by last accessed date or a combination of multiple filters. You can then easily search, or sort, based on text or wild cards. You may have multiple classification rules configured and data tagged with different severity levels to help you adhere to specific compliance regulations or security policies. This will then help you sort the data based upon the compliance requirement you are working towards with flexible reporting around your most sensitive files.

View Who Has Permissions to Your Sensitive Data

Being able to determine current permissions in your File Server helps to ensure that only the right users have access to the right data – which will enable you to enforce a Policy of Least Privilege.

Lepide Data Security Platform enables you to easily uncover and visualize who currently has which permissions to your most sensitive files and folders by comparing applied NTFS and Share Permissions.

Identify How, When and by What Means Access Was Granted

Using the permissions exploration feature, determine by what means and method the access was granted to this data, who granted the access levels and when. A simple way of helping to reduce the risks of permission sprawl on your most important files and folders. This means that, if a user is given excessive permissions to sensitive data (either directly inherited from a parent directory or applied through group membership), you are able to easily identify the effective permissions and the complete scope as to how these permissions are being granted.

Uncover and Compare Historical Permissions to Sensitive Data

Once installed, you will be able to create snapshots of current permissions to allow you to keep a track of historical permissions and compare them with just a few clicks. This gives a complete view of permission evolution through time. Understanding what permissions were applied to sensitive data in the past, what those permissions are today and how the permissions have evolved through that designated window of time.

Explore What a Specific User or Group Has Access to and At What Level

Pick a user or a group and easily drill down to see exactly which files and folders this user can access. You can also see the permission levels

that apply to the specific files and folders to help you maintain control of the levels of permissions to your critical data.

Identify Data ‘At Risk’ By Showing Current Open Shares

A simple report enables you to see a list of all the open shares that exist within your environment, along with the files and folders that reside within them to help ensure you can spot data that is over exposed and needs to be secured down.