



Datasheet

Data Classification

Identify Where Sensitive Data is and Why it is Sensitive

The data discovery and classification software from Lepide helps give you more context around your most sensitive data, so that you easily identify potential areas of exposure and apply the correct access controls. See how many of your files contain sensitive data, where they are distributed, what type of data you have and more.

Improve Data Security

Identify which of your data needs to be the focus of your security strategy, which data is potentially overexposed, which data applies to compliance regulations and address data that is stale.

Easier Compliance Response

Many compliance regulations require you to know exactly where your sensitive data is so that you can easily meet requirements such as the GDPR's access requests and the right to be forgotten.

Remove False Positives

False positives are a common problem many classification tools face. Proximity scanning enables you to filter out false positives from your scan to improve the accuracy of your classification.





How it Works

Incremental Scanning

After an initial discovery and classification scan, data can be classified at the point of creation/modification incrementally to give you a scalable solution that works quickly and efficiently.

Wide Range of File Types

You can scan a wide range of different file types, including word documents, text documents and excel spreadsheets, to find out where your sensitive data resides.

Prioritize Data Based on Risk

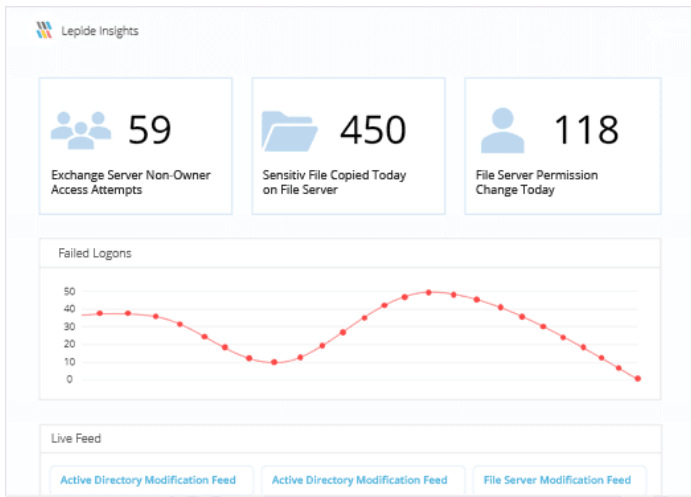
Categorize and score data based on the risk value of the content so that you can focus your user behavior analytics and permissions strategies on the data that matters most

Giving Context to Data Classification

Having more context about what classifications your data falls under enables you to more easily spot suspicious or unwanted user behavior.

Unauthorized permissions changes, anomalous user behavior, multiple failed access attempts, and other signs of data breaches can be captured, reported on and alerted on in real time.

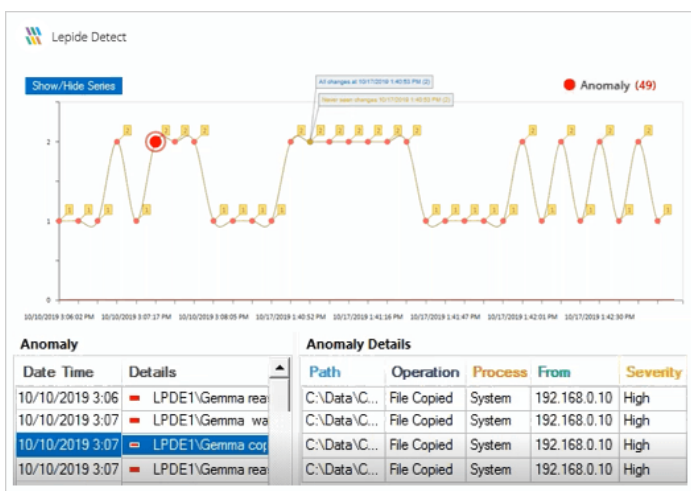
If the worst does happen, you can quickly identify the severity of a breach by determining what types of data were involved.



Use Data Classification to Set Appropriate Access Rights

Easily identify the owners of sensitive files so that you can make better decisions about who should be able to access your sensitive data.

Proactive classification enables you to work towards a model of least privilege, where users only have access to the data they need to do their jobs.

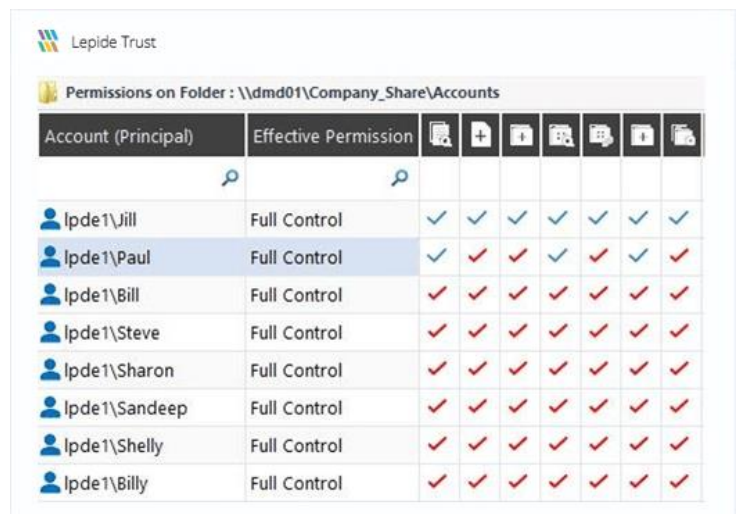


Using Data Classification to Improve Data Security

Having more context about what classifications your data falls under enables you to more easily spot suspicious or unwanted user behavior.

Unauthorized permissions changes, anomalous user behavior, multiple failed access attempts, and other signs of data breaches can be captured, reported on and alerted on in real time.

If the worst does happen, you can quickly identify the severity of a breach by determining what types of data were involved.



The screenshot shows the 'Permissions on Folder' interface for the path '\\dmd01\Company_Share\Accounts'. It lists eight users with 'Full Control' permissions. Each user's permissions are detailed in a grid of checkboxes, with blue checkmarks for 'Jill' and red checkmarks for the others.

Account (Principal)	Effective Permission	Read & execute	Change permissions	Full control	Read & execute	Change permissions	Full control	Read & execute	Change permissions	Full control
lpde1\Jill	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓
lpde1\Paul	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓
lpde1\Bill	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓
lpde1\Steve	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓
lpde1\Sharon	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓
lpde1\Sandeep	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓
lpde1\Shelly	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓
lpde1\Billy	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓

FAQs

What file types are supported?

We support over 85 file types (Including image files). Some of the more popular file types supported are: .doc, .xls, .sxc, .vsd, .rtf, .pdf, .ots, .sti, .txt, .xml, .pps, .stc, .csv, .ods, .ppt, .eml, .sub, .sxw, .aacdb, .dwg, .zip, .rar, .log, .mdb, and more.

How do you handle false positives?

When we search for specific patterns, we take into account the structure of the pattern we are searching for. For example, if a pattern must have a specific sequence of numbers/letters, we will only classify the correctly structured sequence. We also use proximity searching to eliminate false positives by giving the discovered pattern more context on the surrounding phrases/keywords in the file.

Can I search for sensitive data specific to my organization?

Outside of the 100's of predefined rules, there is also the option to easily create your own rules, values and templates for discovery and classification specific to your business needs or requirements.


How do you discover sensitive data?

There are many different pre-defined rules and templates built into the solution that you can enable out of the box. If a pattern is found in the file that matches the rule applied, Lepide will tag and classify the data respectively. We will then index the file for reporting / alerting. The discovery and classification can either be run periodically across the full dataset or on the fly as and when the files are created / modified.

How long does it take?

There are many variables that will determine the length of time it would take to successfully complete a scan, including the size of the dataset, the size of the file, the file types and the number of patterns/rules you have configured the solution to search the data for. We benchmark against industry standards and speeds when it comes to data discovery and classification.





We recommend running a full, deep scan across your data on a periodic basis (monthly or quarterly) and enable classification on-the-fly in the interim. Every time a new file is created/modified, Lepide will scan the files in real time to identify if there has been any newly created sensitive data