Cloudrise

SOLUTION BRIEF
DATA CLASSIFICATION SERVICES

There is too much data to protect it all, so how do you prioritize?

Once you have discovered where all your data resides, the next step is defining its sensitivity so you can handle it securely across the data lifecycle. Cloudrise Data Classification Services maximize the value of your tech, so you stay focused on what data is important and can develop a plan to protect it.

The Challenge

As much as 43% are not able to identify the location of their critical data, with as much as 59% of respondents outsourcing data storage.[1]

54% of data in organizations is unclassified and unlabeled.[2] Because you cannot protect what you don't know you have it can be difficult obtaining funding and resources necessary to secure your data.

Data classification, coupled with data discovery, protection and governance, strengthens downstream controls that can minimize or mitigate potential breaches and their impact. Data classification leads to persistent data risk and sensitivity awareness, which can shorten response and recovery times.

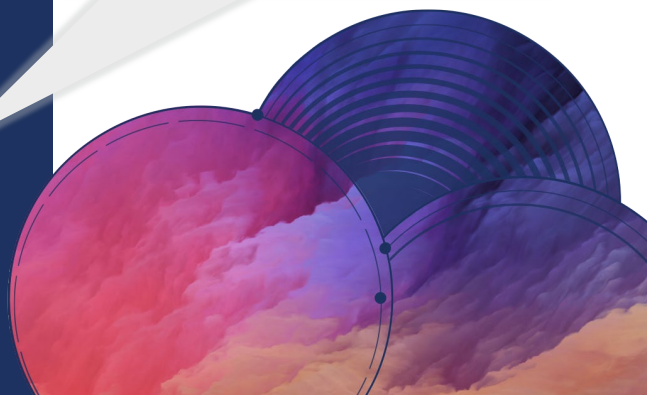
WHEN Data Should Be Classified

Data should be classified as soon as it's created or identified. As data moves through the stages of the data lifecycle, classification should be continually evaluated and updated.

WHY Data Should Be Classified

Classified data provides better insight and control throughout the data lifecycle and enables downstream controls (i.e., DLP, access, handling, etc.) to be more accurate and efficient.

"The real value of data classification is not in labeling data but in understanding the business significance of that data." *- Sunil Soares*



1. *"More than 40% of Companies Don't Know Where their Data is Stored" (Lepide)*
2. *"Problems in information classification: insights from practice" (EmeraldInsight)*

Data classification is the foundation for a comprehensive information security strategy to enhance data awareness and protection within an organization.

Tailored Security

Enables organizations to strategically implement appropriate security measures and controls

Risk Management

Allows for prioritization of protection efforts to focus resources based upon sensitivity and risk exposure

Incident Response

Allows for quick and efficient organizational response in the case of a data breach

Regulatory Compliance

Helps facilitate compliance with regulations by enabling targeted security measures for each data category

Following the Data

Following the data with a classification applied will lead to less friction with access control, DRM, etc.

Downstream Security

Data that is classified correctly will make downstream controls much more accurate and efficient

Supported Technologies

BigID

SPIRION

Microsoft Purview

Our Recommended Approach

Identify

Identify the different data repositories interacting with the information throughout the data life cycle

Prioritize containers of high risk to low (i.e. share drives, databases, web servers)

Discover

Discover the location and accessibility where your sensitive data resides

Determine the effectiveness of existing controls and processes that are derived from data sensitivity

Produce and maintain a data inventory

Classify

Classify data according to its value, type and/or sensitivity in the org (i.e. IP, proprietary, compliance requirements)

Provide persistent classification and protection of articles identified to be sensitive

Employ data handling procedures to reduce risk

Cloudrise

Our perspective is organizations should know the sensitivity of their data and how to handle it securely across its lifecycle. Contact us to assist:

CUSTOMERS: cloudrise.com/contact/ | **PARTNERS:** cloudrise.com/partners/