



DSPM – Delivered.

SOLUTION BRIEF — DATA SECURITY POSTURE MANAGEMENT

43%

of orgs were not able to identify the location of their critical data assets.¹

53%

of companies reported they had over 1,000 sensitive files open to every employee.²

54%

of data in organizations is unclassified and unlabeled.³

1) [Lepide](#) 2) [Varonis](#) 3) [Emeraldinsight](#)

Organizations struggle with the task of knowing where their data resides, posing potential risk to data security and regulatory compliance. 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.

ABOUT DSPM PLATFORMS

The current sweetheart of cybersecurity, “DSPM tools provide visibility regarding where sensitive data is, who has access to that data, how it has been used, and what the security posture of the data stored or application is. It does that by assessing the current state of data security, identifying and classifying potential risks and vulnerabilities, implementing security controls to mitigate these risks, and regularly monitoring and updating the security posture to ensure it remains effective.” ~ *Gartner Peer Insights*

CHALLENGES ORGANIZATIONS FACE



Due to ever-changing and diverse workforce environments, employees are introducing new devices, apps, cloud environments...and DATA every minute of every day. Data Discovery is highly intrusive by design and not all organizations are prepared to CONSUME the sheer volume of data uncovered.

Data classification, coupled with data discovery, protection and governance, strengthens downstream controls that can minimize or mitigate potential breaches and their impact.

There are dozens of DSPM vendors in the marketplace, so it's hard to know where to begin – plus – comprehensive solutions require skilled interpretation and application to keep your data awareness current. **Cloudrise can assist...**

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

Provide persistent classification and protection of articles identified to be sensitive

Employ data handling procedures to reduce risk



Operate

Build a data security governance program that drives your people, processes, and tech – and meets the needs of a diverse data compliance and regulatory landscape.

Continuously optimize and manage the tech

EXPECTED RESULTS



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

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.

SCHEDULE A CALL

Cloudrise security services, coupled with a DSPM platform, are the foundation for a comprehensive information security strategy to enhance organizations' data awareness and protection.

<https://www.cloudrise.com/contact/>

