CONCENTRIC Ai

The ultimate DSPM checklist: How to assess your data security posture

For the modern organization, embracing cloud computing is a double-edged sword. While it promises substantial cost savings, enhanced business agility, and a remarkable boost to productivity, it simultaneously introduces a pair of formidable data challenges:

- Immense growth in how much data an organization must manage
- Massive migration of data to the cloud

From a data protection standpoint, perhaps the most difficult challenge to address is that business-critical data worth protecting now takes so many different forms. From intellectual property to financial data to business confidential information to PII, PCI data and more — creating a complex environment.

Traditional data protection methods, like writing rules to discover what data is worth protecting, simply won't cut it in today's cloud-centric environment. And because it's so easy for your employees to create, modify and share sensitive content with anyone, sensitive data is at risk from data loss.

The truth is, you cannot rely on employees to ensure that data is shared with the right people at all times.

Data security posture management (DSPM) empowers you to identify all your sensitive data, monitor and identify risks to business-critical data, and remediate and protect that information.

With this simple checklist with actionable items, you can audit your cloud data security posture, assess your risk, and take steps to mitigate that

1 DISCOVER/IDENTIFY YOUR SENSITIVE DATA

The first step on the checklist is all about the ability to automatically identify all the data sitting in the cloud. What is so critical here, especially with cloud data, is to recognize that a lot of this data is unstructured. Unstructured data lives in text documents, emails, multimedia files, communication apps, and even social media posts.

That data can be in the form of tax filings, contracts, intellectual property, PII, PCI customer data, trading documents, or operational data.

Variations of your data may be sitting across all your cloud repositories. For example, users may have shadow data sitting in repositories that security teams didn't even know existed.

The most efficient method of discovering where all your sensitive data might be is without rule writing or placing an effective burden on the security teams to do a manual heavy lift upfront.

Action item: *Know where your sensitive data is, whether it's cloud or on-premises, structured or unstructured.*

2 UNDERSTAND THE CONTEXT OF YOUR DATA

The next step on the checklist is still a part of the discovery phase, but it's important enough to take up its own section here. Understanding data with context means knowing your data not just by type (like PII, IP etc.) but the context around the data itself. This includes awareness of applications, networks, data classifications, users and identities, and event types.

Modern DSPM solutions can autonomously do this — with little to no effort required from your security team.

Action item: *Analyze data beyond its type (PII, IP, etc.) by considering the surrounding context, including applications, networks, data classifications, users, identities, and event types.*

3 TRACK AND UNDERSTAND DATA LINEAGE AND PERMISSIONS

This step is all about understanding the issues surrounding sharing entitlements, permissions, location, and activity — and it is crucial to understanding risk.

Here, you'll want to answer several questions. Let's start with an example. Let's say you have 30 versions of a sensitive contract.

The questions you need to answer include:

- How do you know which is the oldest version and which is newer?
- How do you know where all the variations of that particular contract may be residing across your repositories?
- Where are all of these thematically similar data?
- Who has it been shared with?
- Who has access to it? Where is it located?
- Who's actually accessing it regularly?

4 IDENTIFY RISK

Understand where there is risk to sensitive data from:

- Inappropriate permissioning: instances where inappropriate users/groups have access to business critical data
- Wrong entitlements: scenarios where users are granted more privileges or access rights than they require for their roles, posing a potential risk to data security and integrity
- Risky sharing: situations where sensitive data is shared without proper safeguards, potentially exposing it to unauthorized individuals or entities
- Wrong location: instances where sensitive data is stored in unsecured or inappropriate locations, making it more susceptible to unauthorized access or loss
- Abnormal activity: unusual or suspicious actions related to data access or use, which may indicate a potential security threat or data breach

Action item for numbers 3 and 4: *Evaluate sharing entitlements, permissions, location, and activity for sensitive data to determine potential risks. Address*

Note: An effective solution should be able to autonomously identify risk

5 TAKE ACTION AND REMEDIATE THE RISK

Each step in the DSPM process is equally important, but data discovery and data risk monitoring can only take you so far. Taking action based on the discovered risk is crucial.

A robust DSPM solution must investigate and remediate risk and do so proactively. Fixing permissions, changing entitlements, disabling risky sharing and moving data to the right location are all requirements of any effective DSPM solution.

Finally, it all has to happen with a fair degree of accuracy. A DSPM tool is only practical if it provides a low rate of false positives and a low rate of false negatives. When you have too many, you'll spend much more in team resources than you will on data security solutions.

What this means is: a good DSPM solution offers great ROI.

DSPM can empower you with actionable insights without requiring you to have large teams to either manage or administer the systems. With robust DSPM, small teams can be focused on doing what they'd like to do best — interpreting the risk findings and taking action.

Action item: *Choose a robust DSPM solution that accurately detects risks, minimizes false positives and negatives, and offers a strong ROI. It should empower even small security teams to focus on interpreting risk findings and taking timely action.*

REQUIREMENTS FOR AN EFFECTIVE DSPM SOLUTION

Platform	
SaaS	Yes
Private cloud	Yes
Agent based	No
Works out of the box without rules, regex or upfront policy	Yes
Accuracy for PII/PCI	High
Accuracy for all biz critical data (contracts, design docs…)	High
Data Discovery Categorization & Classification	
Rule-less or AI based discovery of PII/PCI with context	Yes
Rule-less or AI based discovery of all biz critical data – contracts, financial docs, NDA, source code, design docs	Yes
Data categorization all biz critical data – PII/PCI, biz confidential data such as contracts, NDA, financial docs, source code	Yes
Classification reliant on end users	No
Central AI based data classification	Yes

CONCENTRIC Ai

REQUIREMENTS FOR AN EFFECTIVE DSPM SOLUTION

Data Risk Monitoring	
Data Risk Profiles	Yes
Data Access Reviews	Yes
Anomaly detection (classification mismatch, entitlement mismatch, sharing mismatch…)	Yes
Data security incident investigation	Yes
Thematic search of data	Yes
Data Remediation	
Auto categorization and classification	Yes
Classification remediation	Yes
Entitlement remediation	Yes
Data Stores Support	
Cloud data stores (O365, Box, Dropbox, Gdrive, S3..)	Yes
On premises data stores (Windows file shares)	Yes
Email/messaging applications	Yes

WHY CUSTOMERS LOVE CONCENTRIC AI FOR DATA SECURITY POSTURE MANAGEMENT

Faced with exponential data growth, massive cloud migration, and increasingly diverse and complex data types, today's modern enterprise is struggling with data security. Protecting intellectual property, financial, business confidential, and regulated PII/PCI/PHI) data in increasingly complex environments can be a monumental challenge.

With Concentric, your organization can:

- Discover, monitor and protect all data types, including Cloud, on-premises, structured, unstructured, and shared via messaging services
- Gain a risk-based view of data and users
- Leverage automated remediation to instantly fix access and activity violations
- Find risk without rules, formal policies, regex, or end-user involvement
- Secure API-based SaaS solution with no agents required

Our solution provides agentless integration with numerous cloud products and services. It's also so easy to deploy — sign up in 10 minutes and see value in days.