Normalyze™

data-first cloud security

DSPM Buyer's guide

Data security posture management

Key points for discovering value in a DSPM solution

Presented by Normalyze Inc.

Contents

Summary 4
Key points 4
Strategic planning assumption 4

Key capabilities of a DSPM solution 5
1. Data discovery 6
2. Data classification 6
3. Access governance 6
4. Detect risks & remediate vulnerabilities and cloud misconfigurations 7
5. Compliance 8

Clarify what each DSPM solution does 9

Benefits of DSPM 10
1. Discover sensitive data 10
2. Classify sensitive data and map it 10
3. Discover attack paths 10
4. Connect with DevOps workflows to remediate risks 10

Technical features evaluation 11
1. Data discovery 11
2. Data classification 11
3. Access governance 12
4. Risk detection 13
5. Remediation 13

Contents

Operator features 14

1. Usability 14
2. Open API 14
3. Integrations 15

Business benefits 16

1. Process control 16
2. Cost effectiveness 16
3. Compliance 17

Supporting materials 18

- Normalyze guide 18
- Normalyze video 18
- Normalyze data sheets 18
- Normalyze case studies 18
- Normalyze blogs 18
- DSPM analyst reports 18
- Normalyze frequently asked questions 18
- About Normalyze 19

Data-first cloud security

Summary

Data Security Posture Management (DSPM) defines a new, data-first approach to securing cloud data. DSPM is based on the premise that data is your organization's most important asset. The proliferation of data in modern multi-cloud organizations is rapidly increasing risks of sensitive data loss or compromise. These risks make cloud data security the **#1 problem** for security stakeholders – especially those using legacy strategies for protection. DSPM charts a modern path for understanding everything that affects the **security posture** of your data. DSPM tells you where sensitive data is anywhere in your cloud environment, who can access these data, and their security posture. Following the guidelines and platform-based instrumentation of DSPM is the quickest way to keep your organization's data safe and secure.

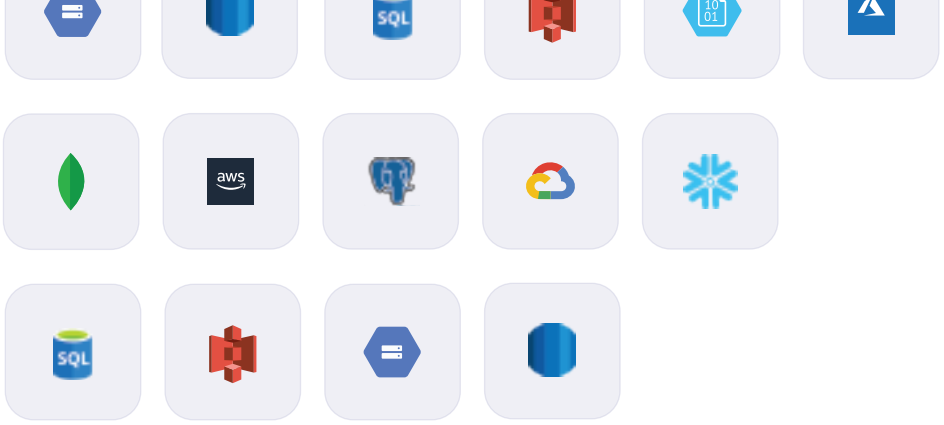
This DSPM Buyer's Guide will help organizations that are considering potential solutions understand how to establish evaluation guidelines, and effectively compare what each solution can or cannot do for meeting operational and business goals.

Key points

- **DSPM is a new term for the cloud security market**, which can confuse evaluators – especially stakeholders coming up to speed on what the technology is and how it can benefit the organization. That's why your evaluation must clearly establish what each solution can do.
- **The entity evaluating DSPM needs to define** what benefits are important for meeting goals of the organization.
- **Evaluators of a DSPM solution will have different perspectives** on what factors are important. This guide will help to clarify the selection criteria before your evaluation proceeds. Industry DSPM criteria are shared for technical features, operator features and business benefits.

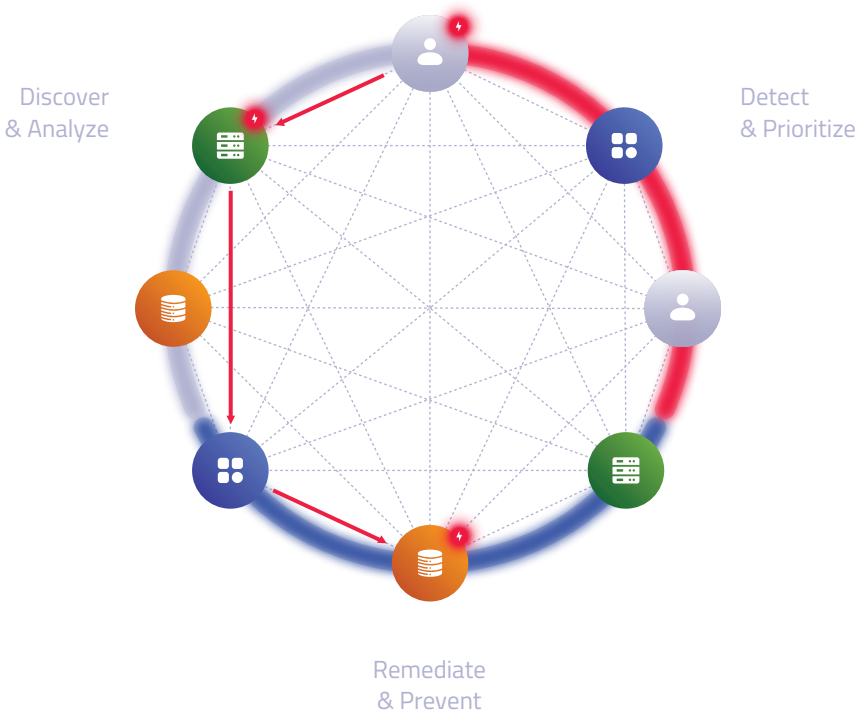
Strategic planning assumption

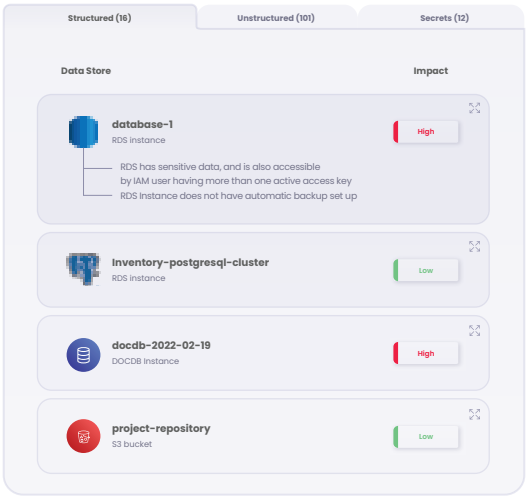
The DSPM evaluation should demystify buzzwords and make it simple for stakeholders to understand what each candidate solution may deliver in terms of meeting relevant requirements weighed by an organization's different stakeholders.



Key capabilities of a DSPM solution

The DSPM platform will automate five domains of capabilities for assessing the security posture of cloud data, detecting and remediating risks, and ensuring compliance. In general, it's useful to look for a DSPM platform that is **agentless** and **deploys natively** in any of the major clouds (AWS, Azure, GCP). The platform should provide **100% API access** to easily integrate the use of any of your existing tools' data required for using DSPM in your organization's environment. Naturally, the platform should also use **role-based access control** to keep the management of data security posture just as secure as the sensitive data should be. All of these will minimize roadblocks and make DSPM quickly productive for your teams.





1. Data Discovery

Discovery capability answers the question, "Where is my sensitive data?" DSPM discovers cloud native **structured and unstructured** data stores. It discovers cloud native **block storage**, such as **EBS volumes**. It discovers PaaS data stores such as **Snowflake** and **Databricks**. DSPM should continuously monitor and discover new data stores. And it should notify security teams on discovery of new data stores or objects that could be at risk.

2. Data Classification

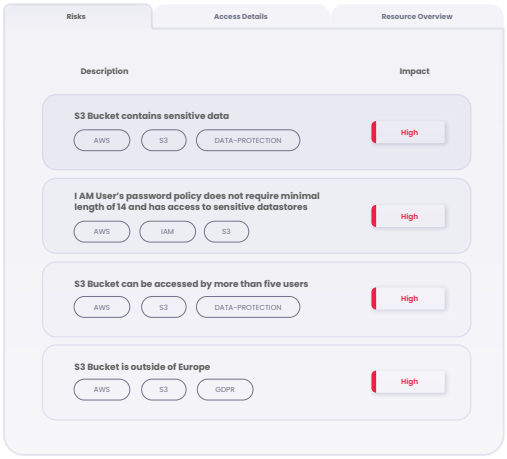
Classification tells you if your data is sensitive and what kind of data it is. It answers questions like "Who can access my data?" and "Are there **shadow data stores**?" First and foremost, you want DSPM classification capability to be automated – if the platform cannot do this automatically, it defeats the whole purpose of trying to do DSPM in massively scaled cloud environments.

3. Access Governance

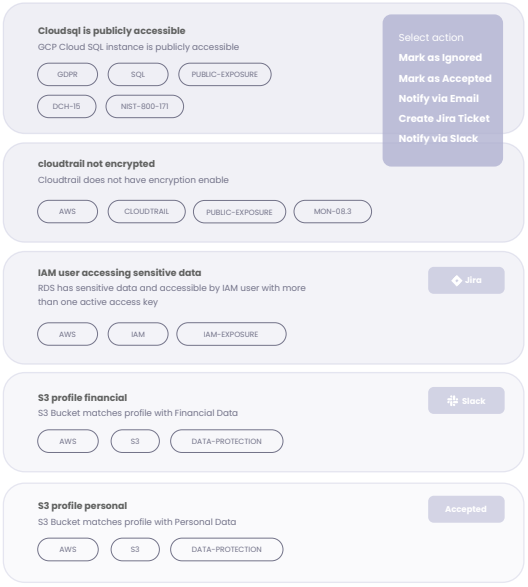
Access governance ensures that only authorized users are allowed to access specific data stores or types of data. DSPM's access governance processes will also discover related issues, such as: "Are there abandoned databases?" or "Are there excessive privileges?" A platform's automated capabilities needs to include identification of all users with access to cloud data stores. It should identify all roles with access to those data stores. DSPM should also identify all resources with access to those data stores. In relation to all of these, the platform also should track the level of privileges associated with each user/role/resource. Finally, DSPM must detect external users/roles with access to the data stores. All this information will inform analytics and help determine the level of risk associated with all your organization's cloud data stores.

4. Detect risks & remediate vulnerabilities and cloud misconfigurations

This domain is about functions of **vulnerability management**. Risk detection is a process of finding potential attack paths that could lead to a breach of sensitive data. Legacy security typically does this by focusing on the infrastructure supporting data (i.e., network gear, servers, endpoints, etc.). DSPM focuses on detecting vulnerabilities affecting sensitive data, and insecure users with access to sensitive data. DSPM also checks data against industry benchmarks and compliance standards such as GDPR, **SOC2**, and PCI DSS.



The main idea is to visually map out relationships across data stores, users, and cloud resources to guide investigation and remediation. The platform should enable building custom risk detection rules that combine sensitive data, access, risk, and configurations.



It should support custom queries to detect and find potential data security risks that are unique to your organization and environment. Security teams should be provided with trigger notifications to specific assignees upon detection of risks. Related workflows should automatically trigger third-party products such as ticketing systems. To ease usability, modern graph-powered capabilities will visualize and enable queries to spot attack paths to sensitive data.

5. Compliance

Modern organizations must comply with a variety of laws and regulations governing sensitive data. For example, the European Union's **General Data Protection Regulation** (GDPR) aims to ensure rights of EU citizens over their personal data such as names, biometric data, official identification numbers, IP addresses, locations, and telephone numbers. A tiered system of fines for non-compliance can be up to 4% of a company's global annual turnover or 20 million Euros (whichever is greater). Similar laws such as the **Health Insurance Portability and Accountability Act** (HIPAA), **Gramm-Leach-Bliley Act** (GLBA), the **Payment Card Industry Data Security Standard** (PCI DSS), and the new **California Consumer Privacy Act** (CCPA) all have mandates for securing specific types of sensitive data. DSPM must be able to automatically detect and classify all data within all your organization's cloud data stores related to any relevant laws and regulations. It should automate mappings of your data to compliance benchmarks.

Stakeholders in your organization should get a coverage heatmap on data compliance gaps, such as misplaced **personally identifiable information** (PII), shadow data, or abandoned data stores with sensitive data. Data officers should receive a dashboard and report to track and manage data compliance by region, function, and so forth. In addition to ensuring security of regulated sensitive data, the platform should also simplify and accelerate producing documentation verifying compliance for auditors.

Clarify what each DSPM solution does

DSPM is a relatively new concept, designed to meet rapidly evolving requirements for securing cloud data. DSPM has entered On the Rise "first position" in Gartner's Hype Cycle for Data Security, 2022. Gartner assigns DSPM a "transformational" benefit rating due to the critical nature of cloud data.

While DSPM is a new concept, subsets of its general functionality are seen in current tools for cloud security. Unfortunately, their functionality is siloed, and these standalone tools do not fulfill all five major functions of DSPM required for systematic, comprehensive, and effective security of all cloud data.

The matrix below shows how current cloud security tools are partially addressing the five functions of DSPM in various types of cloud data stores. Essentially, DSPM fulfills all the squares stating "None" and may replace tools in the other squares – especially if an organization's use cases for particular tools are minimal. Alternately, if an organization has significant investment in particular cloud security tools (such as populating a CMDB with hundreds of thousands of assets, owners, business criticality, etc.), the DSPM platform can also ingest operational data, alerts, and other metrics from your existing infrastructure of corresponding tools for security, IT operations, and DevOps. Use case flexibility goes a long way with DSPM!

Current Cloud Security Tools Fall Short

DSPM functionality	Data discovery	Data classification	Access management	Risk / Vuln management	Compliance
SaaS apps	CASB	CASB	SSPM	CASB	NONE
PaaS databases	NONE	NONE	NONE	NONE	PrivacyOps
IaaS databases	CMDB	PrivacyOps	NONE	NONE	PrivacyOps
IaaS block storage	CMDB	CASB	CIEM	CSPM	PrivacyOps
IaaS file storage	CSPM	NONE	NONE	NONE	PrivacyOps
Coverage	Significant		Partial		NONE

Benefits of DSPM

To help evaluate the utility of a DSPM solution, it's important to distill a simple statement of product benefits that are important for your organization's goals. For example, Normalyze DSPM provides four fundamental benefits that flow from technical capabilities and features of the solution. The candidate solutions can be gauged against these benchmarks to objectively understand if each solution may (or may not) serve your organization's requirements.

1. Discover sensitive data

DSPM discovers **sensitive data** (both structured and unstructured) in your cloud environments, including forgotten databases and shadow data stores.

2. Classify sensitive data and map It

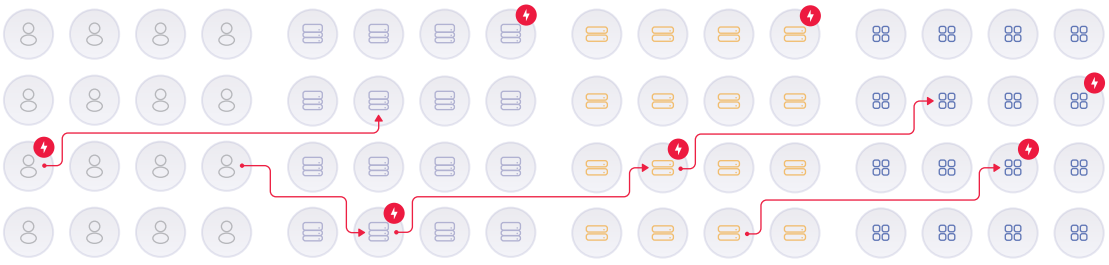
DSPM classifies sensitive data and maps it to regulatory frameworks for identifying areas of exposure and how much data is exposed, and tracking data lineage to understand where it came from and who had access to the data.

3. Discover attack paths

DSPM discovers attack paths to sensitive data that weigh data sensitivity against identity, access, vulnerabilities, and configurations – thus, prioritizing risks on which are most important.

4. Connect with DevOps workflows to remediate risks

DSPM connects with **DevSecOps workflows** to remediate risks, particularly as they appear early in the application development lifecycle.



Technical features evaluation

A core element of a DSPM solution evaluation is weighing the various technical features against requirements of the organization. Below are six categories of DSPM technical capabilities that should be confirmed during each solution evaluation. Note that each section finishes with "Other – specified by user organization." This is a reminder that evaluators should always consider specialized requirements that may uniquely apply to your organization.

1. Data discovery

Find sensitive data wherever it exists in the organization's cloud environment.

	Must-have capabilities	Yes	No
a)	Confirm the product discovers cloud native structured data stores (e.g. Postgres, MySQL, Redshift etc.)		
b)	Confirm the product discovers cloud native unstructured data stores (e.g. S3, Azure Blob etc.)		
c)	Confirm the product discovers cloud native block storage (e.g. EBS volumes)		
d)	Confirm the product discovers data in PaaS data stores including Snowflake and Databricks		
e)	Confirm the product discovers embedded databases deployed directly on cloud compute instances (e.g. MongoDB/SQLServer/Elastic/Oracle deployed on EC2)		
f)	Confirm the product provides continuous monitoring and discovery of new data stores		
g)	Confirm the product notifies security team on discovery of new data stores / databases/tables/columns		
h)	Confirm the product is able to support data stores deployed on-premises		
i)	Other – specified by user organization		

2. Data classification

Classify each type of data found to distinguish degree of sensitivity.

	Must-have capabilities	Yes	No
a)	Confirm the product automatically classifies discovered data stores		
b)	Confirm the product classifies by analyzing actual content in data stores (vs. object/table/column names)		
c)	Confirm the product provides out-of-the-box classifiers without requiring customer-defined rules to start classification		

	Must-have capabilities	Yes	No
d)	Confirm the product identifies regulated data (GDPR, PCI DSS, HIPAA, etc.)		
e)	Confirm the product supports defining proprietary classification rules (for identifying proprietary data unique to the organization)		
f)	Confirm the product provides continuous classification to identify sensitive data in newly added databases/tables/columns		
g)	Confirm the product notifies security team on discovery of new sensitive data		
h)	Confirm the product scans data where it sits without any data leaving the customer environment		
i)	Confirm the product supports sampling data while scanning to reduce compute costs		
j)	Confirm the product can detect sensitive data that combines proximity of sensitive data to increase accuracy		
k)	Confirm the product provides workflow to fix false positives when sensitive data is miscategorized		
l)	Confirm the product is able to assess the monetary impact associated with breach of data store based on sensitivity of data involved		
m)	Other – specified by user organization		

3. Access governance

Access governance ensures that only authorized users are allowed to access specific data stores or types of data

	Must-have capabilities	Yes	No
a)	Confirm the product identifies all users with access to cloud data stores		
b)	Confirm the product identifies all roles with access to cloud data stores		
c)	Confirm the product identifies all resources with access to cloud data stores		
d)	Confirm the product tracks level of privileges associated with each user/role/re-source		
e)	Confirm the product detects external (cross-account) users & roles with access to cloud data stores		
f)	Confirm the product can provide a detailed access & privilege report for all users across all cloud data stores		
g)	Confirm the product is able to identify inactive privileges by tracking last accessed date		
h)	Other – specified by user organization		

4. Risk detection

Risk detection is a process of finding potential attack paths that could lead to a breach of sensitive data (a function of vulnerability management, or VM).

	Must-have capabilities	Yes	No
a)	Confirm the product detects potential attack paths that could lead to a breach of sensitive data		
b)	Confirm the product detects vulnerabilities in databases containing sensitive data		
c)	Confirm the product checks detected risks against industry benchmarks and compliance standards (GDPR, SOC2, PCI DSS, CIS, etc.)		
d)	Confirm the product enables building custom queries to detect/find potential data security risks unique to an organization's cloud environment		
e)	Confirm the product enables building custom risk detection rules that combine sensitive data, access, risk and configurations		
f)	Confirm the product eases detection of risks and attack paths by visually mapping out relationships across data stores, users and cloud resources for ad hoc investigation		
g)	Confirm that product is able to detect risk posture of assets/resources (e.g. configuration of compute instances, serverless functions, IAM configurations, risky users) in the cloud that created risk of sensitive data exposure		
h)	Other – specified by user organization		

5. Remediation

Remediation is the process of fixing misconfigurations, deleting shadow data stores, correcting access rights, and other steps to eliminate or minimize risks to sensitive data.

	Must-have capabilities	Yes	No
a)	Confirm the product sends trigger notifications to assignees on risk detection		
b)	Confirm the product triggers workflows in 3rd party products (e.g., ticketing systems, notification tools, automation workflows)		
c)	Confirm the product provides graph-powered guidance to visualize and query attack paths to sensitive data		
d)	Confirm the product can provide detailed remediation steps for each risk.		
e)	Confirm the product can automate bulk remediation based on tags, risk, etc.		
f)	Other – specified by user organization		

Operator features

Operators are the daily users of a DSPM solution. They will have keen interest in comparing how the candidate DSPM solutions really work from a usability and job role execution perspective. Suggestions below will help point your evaluation toward the right path for discovering if a DSPM solution will be right for your organization's operational teams.

1. Usability

Usability is about a DSPM solution's ease of deployment and use as a tool for protecting sensitive data.

	Must-have capabilities	Yes	No
a)	Confirm the product is agentless for easy cloud native deployment		
b)	Confirm the product supports all major cloud service providers (AWS, Azure, GCP)		
c)	Confirm the product allows scanning for an unlimited number of accounts		
d)	Confirm the product's menu command structure is logical and provides quick access to features and information on data security posture		
e)	Confirm the product has graph-based features to accelerate finding sensitive data, detecting and remediating risks, and reporting data security posture		
f)	Confirm the product's user interface is easy to search for risks and attack paths		
g)	Confirm the product provides role-based access control		
h)	Confirm the product provides clear and useful reports on data security posture for all related roles in the organization		
i)	Other – specified by user organization		

2. Open API

An open API architecture allows a DSPM solution to enable integrations with external products.

	Must-have capabilities	Yes	No
a)	Confirm the product supports open APIs, which can be easily integrated with 3rd party solutions to bring their data into the DSPM solution graph		
b)	Confirm the product allows any data seen on the UI to be accessible via APIs		
c)	Confirm the product can use out-of-the-box webhooks to enable outbound integrations with ticketing and notification solutions		
d)	Confirm the product can bring in other data sources (vulns, configs, etc.) into its graph to enrich it		
e)	Other – specified by user organization		

3. Integrations

Integrations allow a DSPM solution to provide enhanced functionality by exchanging security posture data with external applications.

	Must-have capabilities	Yes	No
a)	Confirm the product can import data catalogs from other data management tools and integrate the data into its entity/profiling technique to retain format of the sensitive data		
b)	Confirm the product provides out-of-the-box connectors to integrate popular data stores (e.g., Snowflake, Databricks)		
c)	Confirm the product integrates with ITSM tools like Jira, ServiceNow, etc		
d)	onfirm the product integrates with notification tools like Slack, email, etc.		
e)	Other – specified by user organization		

Business benefits

Business benefits go beyond revealing how a DSPM solution will improve cloud data security posture; they are also intrinsic to how the business may benefit. Try to associate specific metrics with these points as quantifiable benefits will help pass the scrutiny of the CFO and other financial stakeholders – and result in approval of a purchase order for the best DSPM solution

1. Process control

Process control of data security posture enabled by a DSPM solution provides visibility, control and trust.

	Must-have capabilities	Yes	No
a)	Confirm the product provides clear visibility on where sensitive data resides in the organization's cloud environment		
b)	Confirm the product provides clear visibility on risks and attack paths to sensitive data in the organization's cloud environment		
c)	Confirm the product provides control of knowing who has access to sensitive data and if related privileges create risk to data security posture		
d)	Confirm the product can be trusted by never copying or moving sensitive data outside the organization's cloud environment		
e)	Other – specified by user organization		

2. Cost effectiveness

Cost effectiveness by a DSPM solution delivers quantifiable monetary benefits.

	Must-have capabilities	Yes	No
a)	Confirm the product minimizes compute time via an efficient scanning methodology that scans data in-place and sends metadata for analytics		
b)	Confirm the product can eliminate needing to use one or more other data security solutions		
c)	Confirm the product can reduce time required to produce compliance reports for auditors and data officers		
d)	Other – specified by user organization		

3. Compliance

Compliance benefits entail simplifying and accelerating creation of reports for auditors, data officers and executives.

	Must-have capabilities	Yes	No
a)	Confirm the product provides a coverage heatmap on data compliance gaps (misplaced PII, shadow data, abandoned data stores with sensitive data, etc.)		
b)	Confirm the product provides an executive dashboard and reports for data officers to track/manage data security compliance by region, function, etc.		
c)	Confirm the product provides automated mappings to compliance benchmarks (CIS, HIPAA, PCI DSS, etc.)		
d)	Other – specified by user organization		

Supporting materials

The DSPM evaluation can be accelerated by having solution providers give the team associated collateral such as educational videos, architectural diagrams, data sheets, etc. Some collateral will be beneficial for informing non-technical stakeholders about respective solutions from a high level, while others will support deeper technical comparisons. Below are examples of supporting materials from Normalyze:

- **Normalyze Guide**
  Definitive Guide to Data Security Posture Management
- **Normalyze Video**
  Normalyze CEO Interview / Product Background
- **Normalyze Data Sheets**
  Company Backgrounder
  Normalyze Cloud Platform
- **Normalyze Case Studies**
  Corelight transforms data security with Normalyze
- **Normalyze Blogs**
  Blogs
- **DSPM Analyst Reports**
  Gartner Hype Cycle for Data Security, 2022
- **Normalyze Frequently Asked Questions**
  FAQs

About Normalyze

Normalyze is a pioneering provider of cloud data security solutions helping customers secure their data, applications, identities, and infrastructure across public clouds. With Normalyze, organizations can discover and visualize their cloud data attack surface within minutes and get real-time visibility and control into their security posture including access, configurations, and sensitive data to secure cloud infrastructures at scale. The Normalyze agentless and machine-learning scanning platform continuously discovers resources, sensitive data and access paths across all cloud environments. The company was founded by industry veterans Ravi Ithal and Amer Deeba and has a fast-growing customer base across a wide-range of industries, including: Corelight, Chargepoint, Sigma Computing, Netskope, and Orkes. The company is funded by Lightspeed Venture Partners and Battery Ventures. For more information, please visit **normalyze.ai.**

Data-first cloud security

Normalyze™

data-first cloud security