Normalyze™

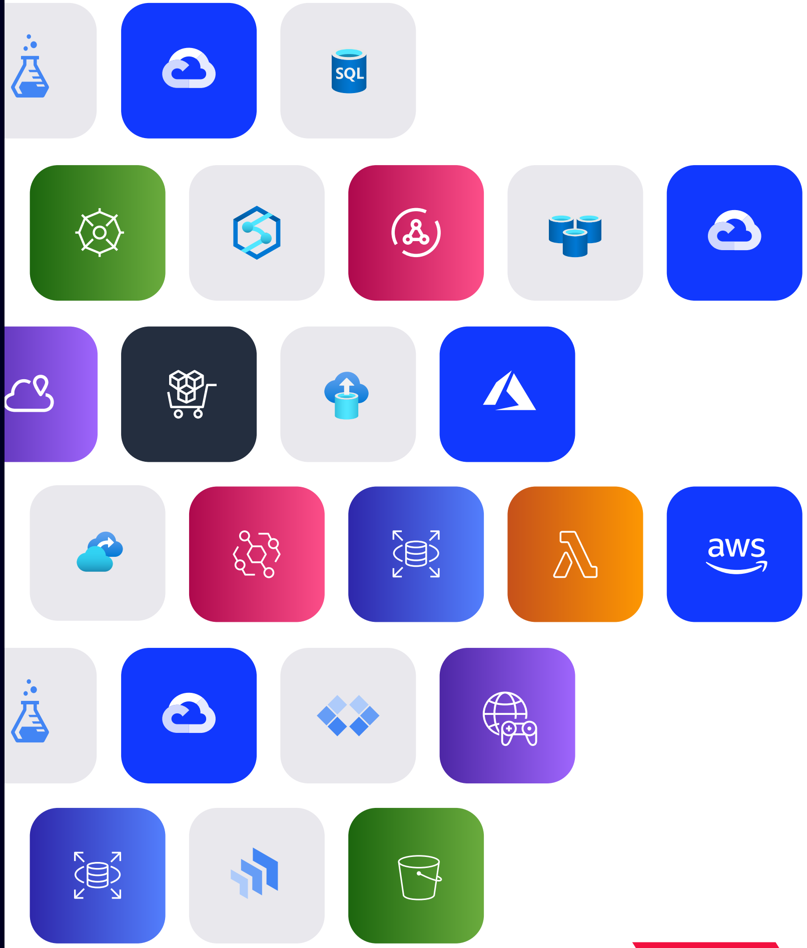
data-first cloud security

# The definitive guide to data security posture management (DSPM)

eBook from Normalyze

# Contents

Data-first cloud security



# What is DSPM?

**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 keeping your organization's data safe and secure.

In this guide, you will learn about capabilities and requirements for DSPM to help your organization create strategy and tactics for addressing cloud data security posture with a systematic, comprehensive, and effective process.

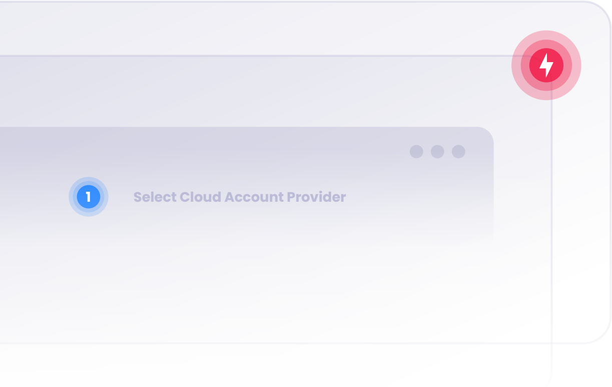
# How can DSPM help you?

**The most important benefit of DSPM is accelerating your organization's ability to continuously keep its cloud data safe and secure.** Assessing and acting on data security posture is different from other types of security posture, such as issues affecting the general cloud, applications, network, devices, identity, and so forth. Unlike these, DSPM focuses like a laser beam on your data.

## Specific benefits of DSPM

As part of keeping your cloud data safe and secure, DSPM specifically will help your security, IT operations, and DevOps teams to:

- **Discover** sensitive data (both structured and unstructured) in your cloud environments, including forgotten databases and shadow data stores.
- **Classify sensitive data and map 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.
- **Discover attack paths** to sensitive data that weigh data sensitivity against identity, access, vulnerabilities, and configurations – thus, prioritizing risks based on which are most important.
- **Connect with DevSecOps workflows to remediate risks**, particularly as they appear early in the application development lifecycle.



# A modern DSPM platform automates the process

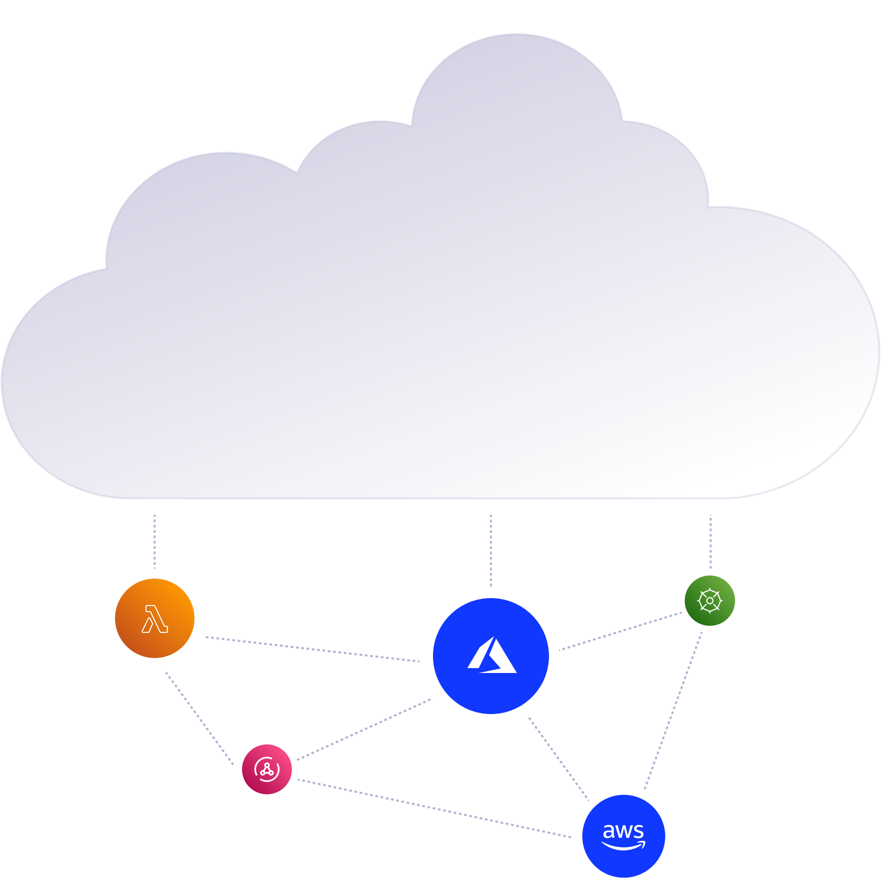
Frankly, the challenge of securing multi-cloud data surmounts purely manual efforts to implement and maintain DSPM processes for various teams of enterprise stakeholders. If your organization desires the benefits of DSPM (and it should!), automated systems are mandatory to ensure DSPM processes are systematic, comprehensive, and effective.

The automation of DSPM entails use of a DSPM platform. A modern DSPM platform has one major focus: to quickly and accurately assess security posture of your organization's cloud data and ensure rapid remediation of vulnerabilities – both for security of the data and for compliance mandates covering various types of sensitive data.

The DSPM platform will not replace existing security tools used for posture management of the network, applications, clouds, and so forth. Indeed, the DSPM platform should and must ingest contextual data, alerts, and other metrics from your existing infrastructure of tools for security, IT operations, and DevOps. These data are crucial for informing the DSPM platform of your entire data infrastructure as it relates to security and compliance. The data fuel algorithmic analysis and processes using artificial intelligence and machine learning (AI/ML) to automatically accomplish what subject matter experts are unable to achieve with manual efforts alone.

The DSPM platform also must seamlessly integrate with security and operational services from all your organization's cloud service providers. These shall include major providers such as Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP). In general, whilst security and operational tools provided by a cloud service provider may be effective within the provider's cloud, interoperability with data security-focused systems in other clouds is poor to non-existent. For this reason, a DSPM platform is mandatory for systematic, comprehensive, and effective cloud data security posture management integrated across the extended cloud environment.

# How does DSPM work?



**One of the biggest questions for cybersecurity is, “Where is our data?”** You can’t begin to secure data until you know where it is – especially critical business, customer, or regulated data. As we’ve learned in this new era of agile, your data can be almost anywhere in the cloud. Getting better visibility is the first step to a process of securing cloud data called Data Security Posture Management.

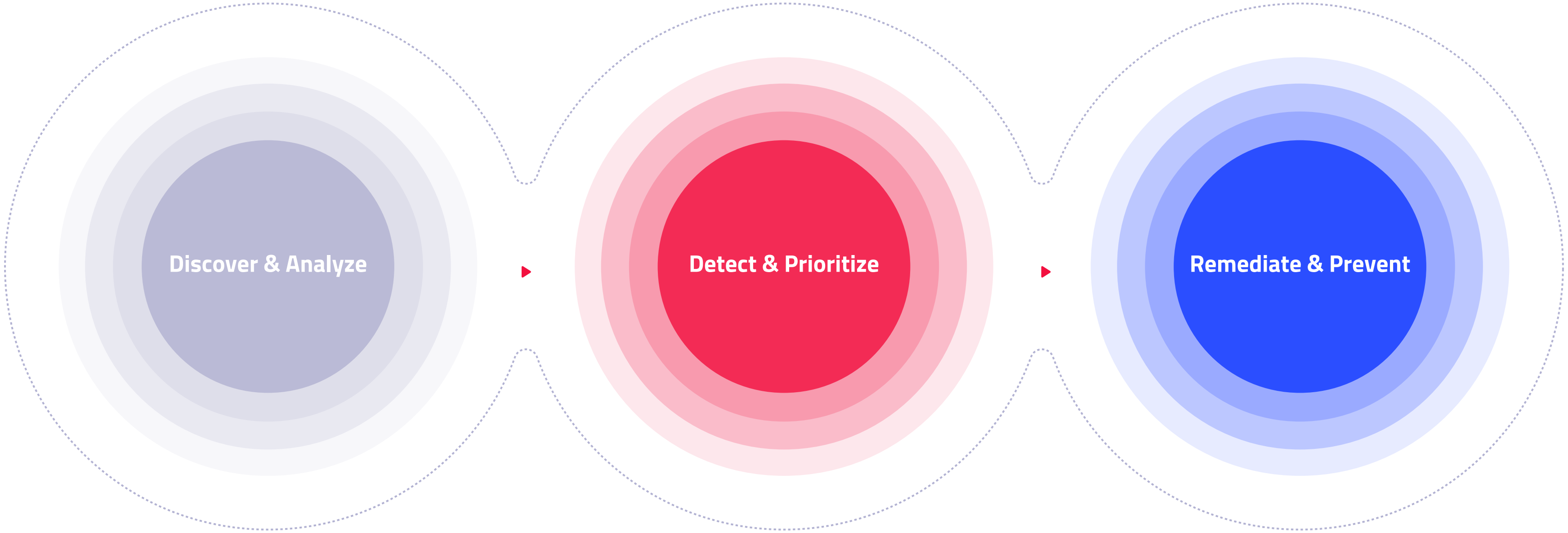
The analyst and vendor communities describe various types of posture management. They all address two general questions: What are the issues, and how can we fix them? Data Security Posture Management (DSPM) is a new prescriptive approach for securing cloud data and defined by Gartner in its **Hype Cycle for Data Security, 2022.**

> Data security posture management (DSPM) provides visibility as to where sensitive data is, who has access to that data, how it has been used and what the security posture of the data store or application is. This requires a data flow analysis to determine the data sensitivity. DSPM forms the basis of a data risk assessment (DRA) to evaluate the implementation of data security governance (DSG) policies.”
>
> **– Gartner**

# Essence of DSPM

Data-first cloud security

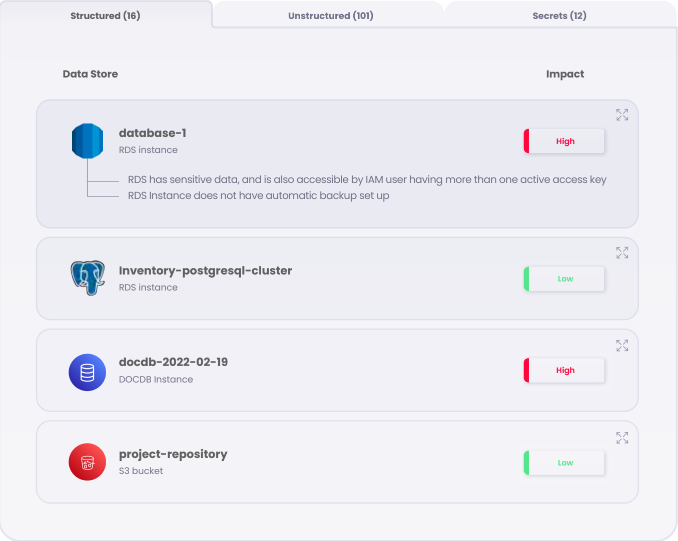
# Essence of DSPM



Discover where your cloud data is and analyze what it consists of

Detect which data is at risk prioritize order of remediation by mapping uset access against specific datasets, and tracking data lineage to understand to understand  where it came from and who had access to the data

Remediate vulnerabilities and prevent their reoccurrence



| Data Store | Impact |
|---|---|
| database-1<br>RDS instance<br>RDS has sensitive data, and is also accessible by IAM user having more than one active access key<br>RDS Instance does not have automatic backup set up | High |
| Inventory-postgresql-cluster<br>RDS instance | Low |
| docdb-2022-02-19<br>DOCDB Instance | High |
| project-repository<br>S3 bucket | Low |

## Phase 1:

# DSPM discovers where your data is and analyzes what it consists of

Discovery of data location is a huge issue because of the nature of agile. In DevOps and model-driven organizations, there is a vastly larger and expanding amount of structured and unstructured data that could be located almost anywhere.

In legacy scenarios, all the data was stored on premises, which spawned the “Castle & Moat” network security model of restricting external access while allowing internally trusted users. Those were the easy days of security! Cloud has fragmented the legacy architecture by storing data at external locations operated by service providers and other entities. For security architects and practitioners, and those responsible for compliance, this titanic shift in data volumes and locations calls for a different approach to securing the data: hence Data Security Posture Management.

The DSPM approach acknowledges that agile architectures are far more complex because the cloud is not a monolithic place. For most enterprises, cloud encompasses many physical and virtual places: two or more cloud service providers such as Amazon, Microsoft, or Google; software-as-a-service providers; platform and infrastructure-as-a-service providers; data lake providers; business partners; and, of course, a myriad of hybrid clouds, servers, and endpoints within your own organization.

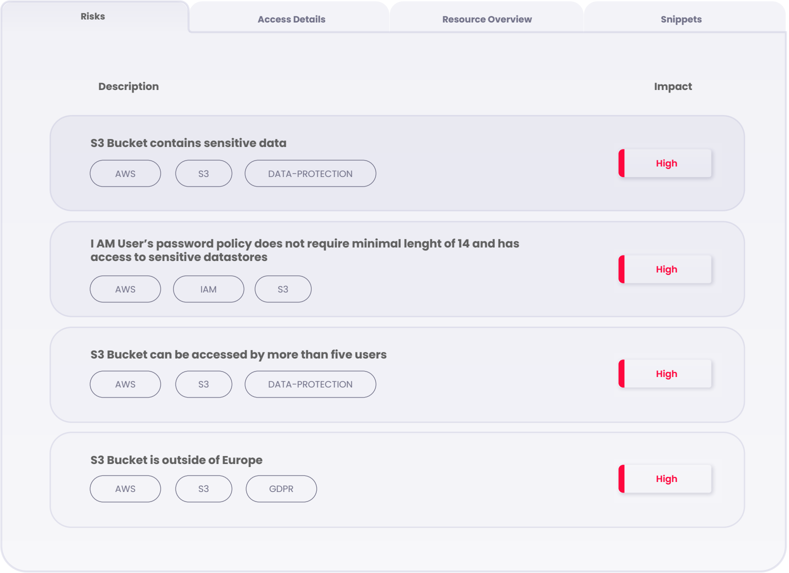
Data isn’t just moving to more places. The velocity of data creation is soaring with a modern explosion of microservices, growing frequency of changes, acceleration of access for modeling, and constant iterations of new code by DevOps. Some of the fallout for security includes shadow data stores and abandoned databases, which lure attackers like honey draws bees.

Locating your data is just the beginning. Classification analysis is needed to help your team understand the nature of the data, and to determine levels of concern as to data requirements for protection and monitoring – especially if the data is subject to compliance mandates.

## Phase 2:

# DSPM detects which data is at risk and prioritizes order of remediation

The second phase of the DSPM is detecting which cloud native data are at risk. A precursor is identifying all systems and related operations running in your organization's cloud environment. Detecting all infrastructure helps determine what all the access paths are to your data and which paths may require access permission changes or new controls for protection.



| Description | Impact |
|---|---|
| S3 Bucket contains sensitive data<br>AWS<br>S3<br>DATA-PROTECTION | High |
| I AM User's password policy does not require minimal lenght of 14 and has access to sensitive datastores<br>AWS<br>IAM<br>S3 | High |
| S3 Bucket can be accessed by more than five users<br>AWS<br>S3<br>DATA-PROTECTION | High |
| S3 Bucket is outside of Europe<br>AWS<br>S3<br>GDPR | High |

The issue of access rights is challenging because structured and unstructured data can be found in many types of receptacles. Examples are cloud native databases, block storage, and file storage services. For each of these, your team will need to spot access misconfigurations, inflated access privileges, dormant users, vulnerable applications, and exposed resources with access to sensitive data.

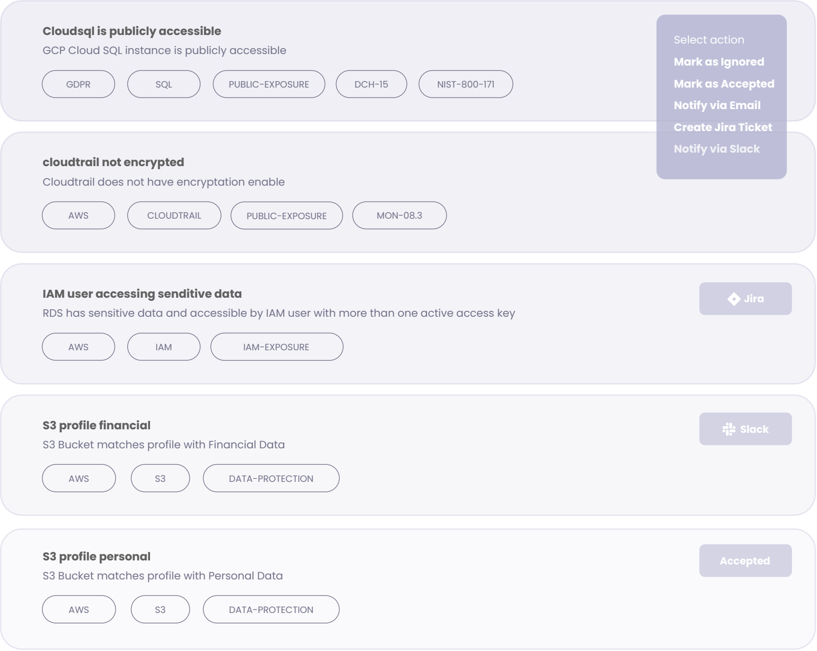
If your organization is coming up to speed on these issues, be aware that security teams must closely collaborate with data and engineering teams due to rapidly evolving cloud application architectures, and by changes to microservices and data stores.

Access is not the only issue for risk; so is the nature of the data. Your teams will need to prioritize the cloud data to enable ranking its importance and risk level. Is the data proprietary, regulated, or otherwise sensitive in nature? Determination of risk is a composite of vulnerability severity, nature of the data, its access paths, and condition of its resource configurations. Higher risk means remediation becomes Priority One!

## Phase 3:

# DSPM remediates data risks and prevents their recurrence

Securing the cloud data at risk entails remediating the associated vulnerabilities discovered during the Discovery and Detection phases of DSPM. In legacy scenarios, data security often focused on securing the classic perimeter. But since data has moved vastly beyond this quaint antiquity, it requires addressing a different scope of issues. As mentioned, remediation will frequently need collaboration by a cross-discipline team. Depending on scenarios, the team will need help with network and infrastructure operations, cloud configuration management, identity management, databases, DevOps, and more.



**Cloudsql is publicly accessible**
GCP Cloud SQL instance is publicly accessible

**cloudtrail not encrypted**
Cloudtrail does not have encryptation enable

**IAM user accessing senditive data**
RDS has sensitive data and accessible by IAM user with more than one active access key

**S3 profile financial**
S3 Bucket matches profile with Financial Data

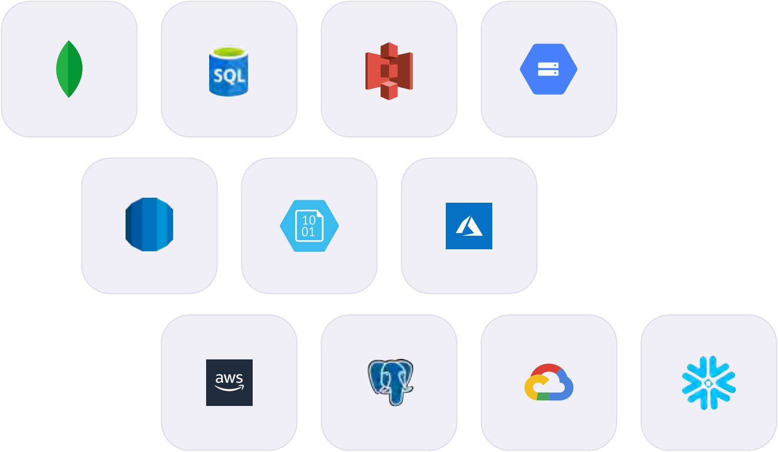
**S3 profile personal**
S3 Bucket matches profile with Personal Data

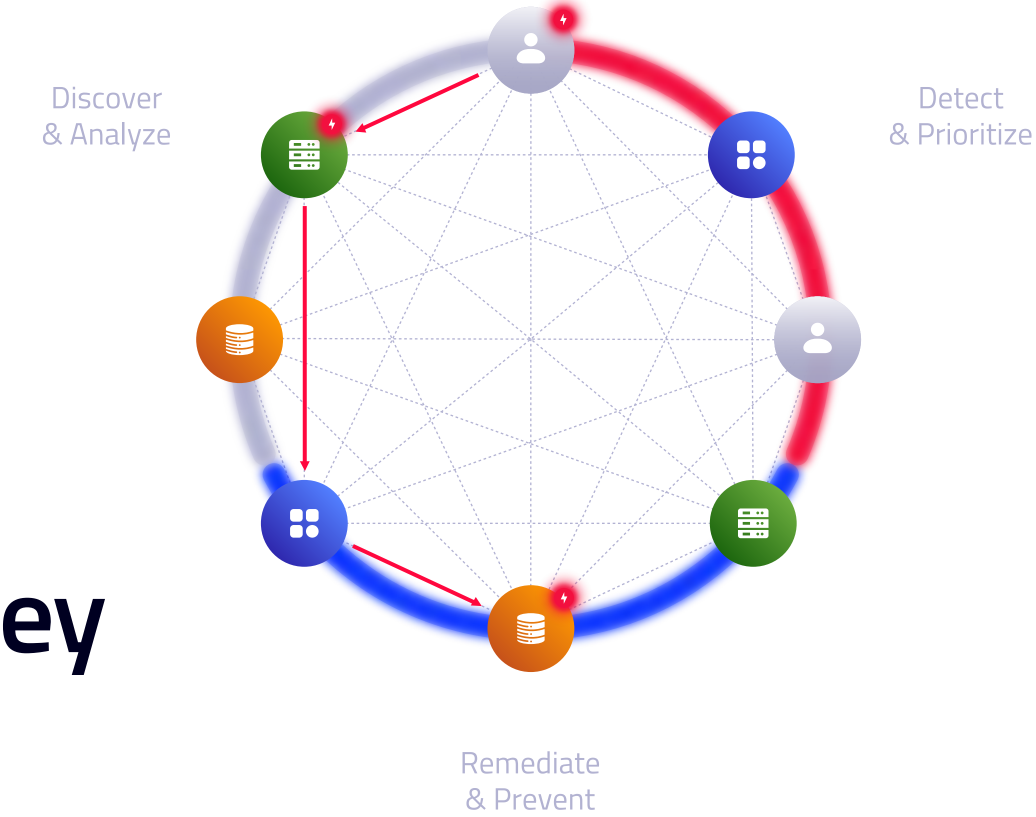
Security of cloud data is usually governed with controls provided by a particular service provider. However, the enterprise subscriber also shares a critical role in addressing several issues mostly related to configuration management:

- Identify where workloads are running
- Chart relationships between the data and cloud infrastructure and related business processes to discover exploitable paths
- Verify user and administrator account privileges to find people with over privileged access rights and roles
- Inspect all public IP addresses related to your cloud accounts for potential hijacking

Since the major cloud service providers do not provide integrated, interoperable security and configuration controls for disparate clouds, it's on your organization to ensure that security access controls are properly configured for multi-cloud environments.

While remediation is the last of a three-step process for DSPM, take note that all three steps are really part of a continuous cycle. When your enterprise relies on the cloud, it's vital to always be on top of data security posture!





# What are the key capabilities of DSPM?

**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 (e.g. 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.

## Data discovery with DSPM

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.

## Data classification with DSPM

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. Automation must address a variety of classification capabilities:

- **Analyze actual content in data stores (vs. object/table/column names).**
- **Provide classifiers out of the box (no customer-defined rules required; this slows you down!).**
- **Identify regulated data (GDPR, PCI DSS, HIPAA, etc.)**
- **Allow user definition of classifiers for proprietary / unique data.**
- **Have classification identify sensitive data in newly added databases/tables/columns.**
- **Notify security team on discovery of new sensitive data**
- **Scan data where it sits without any data leaving your organization’s environment.**
- **Sample data while scanning to reduce compute costs.**
- **Detect sensitive data that combines proximity of sensitive data to increase accuracy.**
- **Workflow to fix false positives when sensitive data is miscategorized.**

## Access governance with DSPM

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.

## Detect risks & remediate vulnerabilities and cloud misconfigurations with DSPM

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.

# Compliance with DSPM

**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.

# Where does DSPM fit into the modern data security environment?

> This is an urgent problem that is encouraging rapid growth in the availability and maturation of this technology.”
>
> **– Gartner**

**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 most important benefit of DSPM is accelerating your organization’s ability to continuously keep its cloud data safe and secure. Assessing and acting on data security posture is different from other types of security posture, such as issues affecting the general cloud, applications, network, devices, identity, and so forth. Unlike these, DSPM focuses like a laser beam on your data.

The matrix on the following page 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 |

The matrix 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. Alternately, DSPM may also ingest operational data, alerts, and other metrics from your existing infrastructure of corresponding tools for security, IT operations, and DevOps.

# How is DSPM being used?

**DSPM is primarily used by cloud-first organizations that put the entire IT/application infrastructure into one or more clouds.** DSPM is also useful for entities that have committed to a cloud-first vision and are migrating from a hybrid cloud/on-premises environment. The practical, day-to-day use of a DSPM platform is illustrated below by four typical use cases.

## Use case 1:

### Automate data discovery and classification across all clouds

Shadow data stores and abandoned data stores often rest outside regular security controls, especially if they are ad hoc duplications made by data scientists and other data engineers for temporary testing and other purposes. This DSPM use case especially benefits security teams by staying in lock step with data and engineering teams to automatically discover, classify, and validate all data across all cloud accounts. The process includes inventorying structured and unstructured data across native databases, block storage, and file storage services.

## Use case 2:

### Prevent cloud data exposure and minimize the attack surface

Organizations pursue a cloud-first strategy because it enables innovation – and this brings a constant evolution of cloud architectures and changes to microservices and data stores. Security teams use DSPM to stay in lock step with data and engineering teams to ensure cloud data exposure is minimized along with the associated attack surface. The DSPM platform will enable automatic identification of data at risk by continuously checking data stores and associated resources for misconfigurations, detecting vulnerable applications and exposed resources with access to sensitive data.

## Use case 3:

### Track data access permissions and enforce least privilege

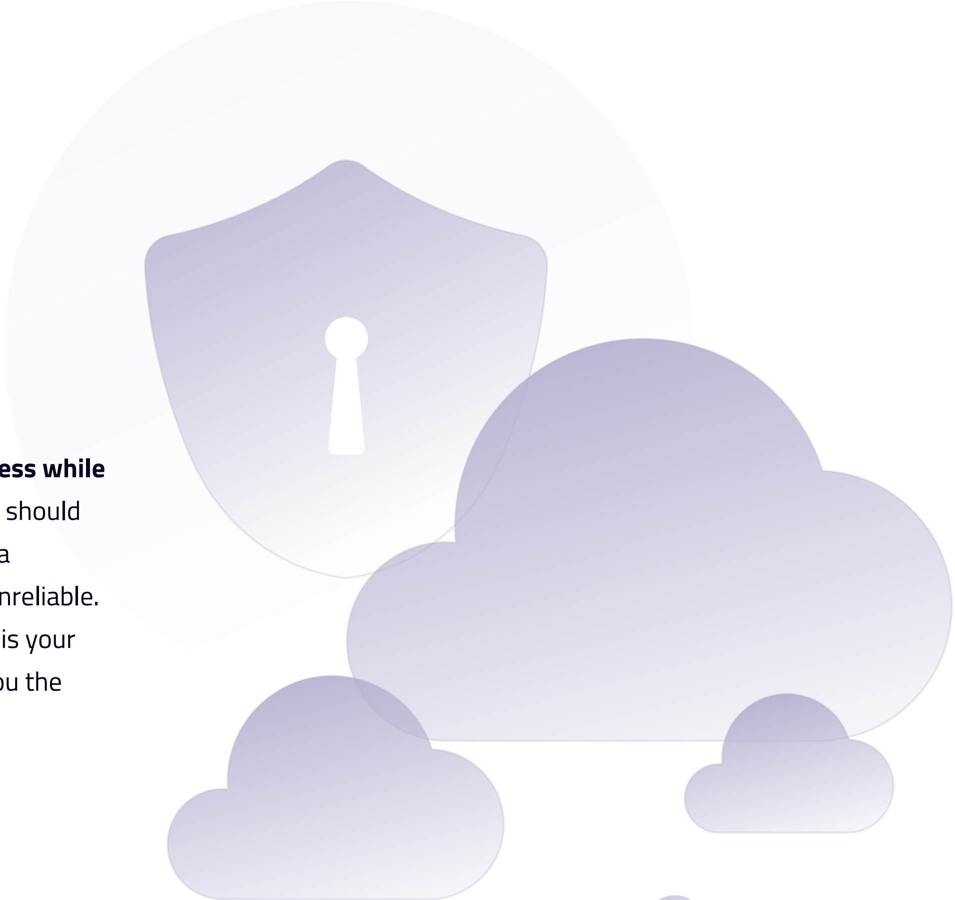
Inappropriate access permissions enable the potential misuse or exposure of sensitive data, either by an insider's accident or design of a nefarious rights-holder. DSPM enables security teams to automatically get a simple, accurate view of access privileges for all cloud data stores. The DSPM platform catalogs all users' access privileges and compares these against actual usage to identify dormant users and those with excessive privileges. The resulting to-do list allows IT administrators to quickly correct excessive privileges or otherwise expunge dormant users whose accounts pose potential risk to the data.

## Use case 4:

### Proactively monitor for compliance with regulations

Compliance audits for data security occur for a variety of mandated laws and regulations. The DSPM platform enables governance stakeholders with the ability to stay ahead of compliance and audit requirements via continuous checks against key benchmarks and associated controls. For example, PCI DSS Requirement 3 specifies that merchants must protect stored payment account data with encryption and other controls. The DSPM platform will identify stored payment account data and whether it is encrypted. Compliance activity like this is enabled by the platform's cloud data catalog, access privilege intelligence, and risk detection capabilities – all of which illustrate sensitive data security posture and provide evidence for compliance audits.

# Why do I need DSPM?

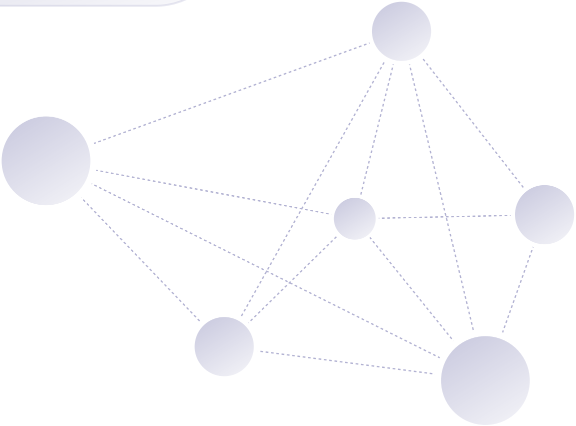


**“Castle & Moat” is the classic model of cybersecurity, which restricts external access while allowing internally trusted users.** While familiarity breeds comfort, security leaders should start feeling very uncomfortable with this business-as-usual approach. We’ve seen a never-ending stream of successful attacks and data breaches, so Castle & Moat is unreliable. It’s also misplaced because attackers aren’t going after your castle. Their real target is your data – and in these days of agile, that could be almost anywhere! And, what gives you the comfort the attackers are not already inside the castle?

Here are six reasons why you should consider putting data at the center of security strategy instead of relying on a legacy Castle & Moat approach.

## » 1. CI/CD brings an explosion of deployments and new changes

The constant change in business requirements has fueled the need for automating stages of application development. Continuous integration and continuous delivery (CI/CD) accelerate app development and make multiple changes to a codebase on a frequent basis. The risk of bugs in apps and data leakage rises with the continuous flow and higher velocity of services and changes because there’s no time for manual review. Cloud data is especially at risk with DevOps constantly spinning up instances and links to data repositories—especially with temporary buckets or forgotten copies of data used for testing apps.



## » 2. AI/ML fuels the need for more access to data for modeling

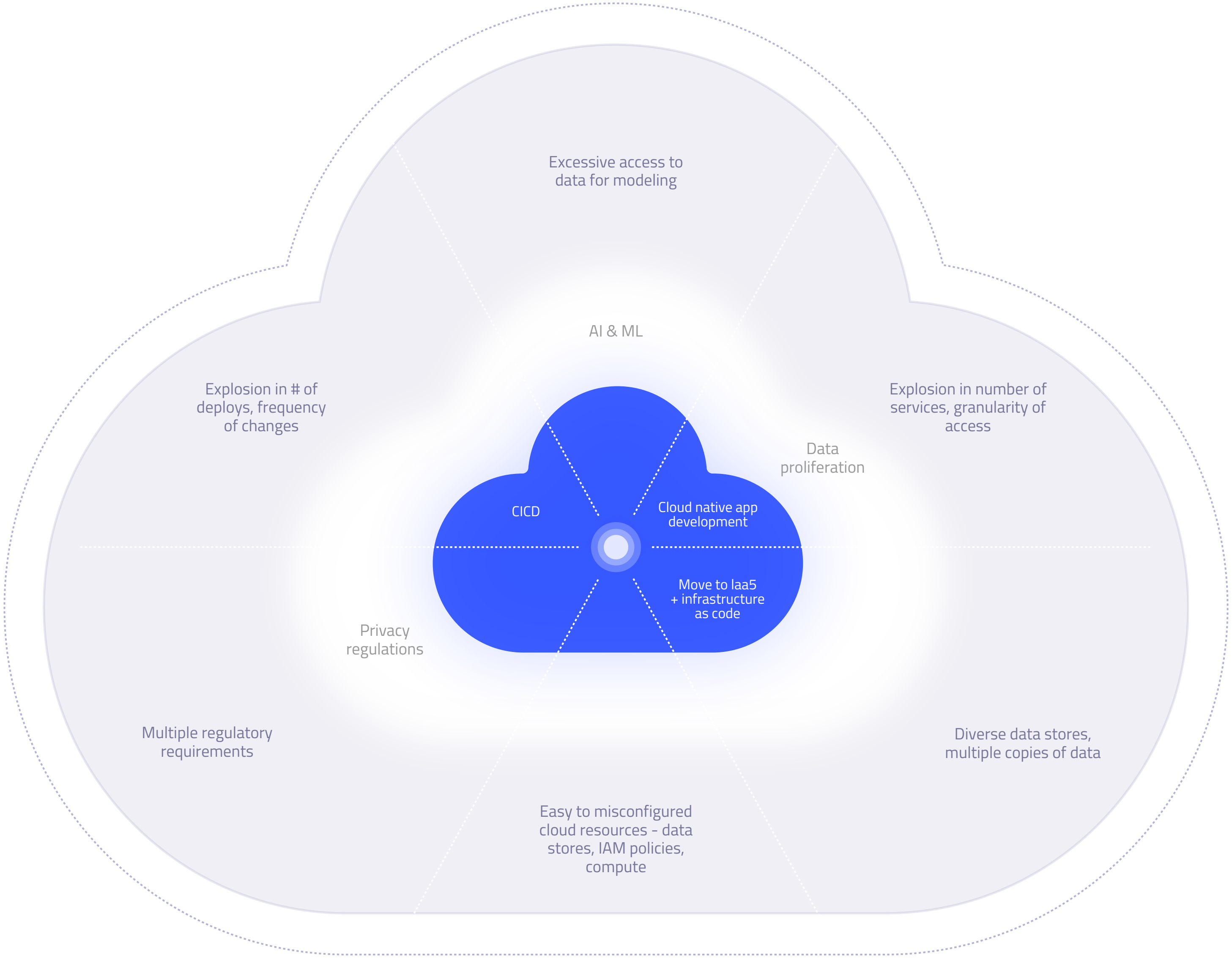
Compared to legacy apps, machine learning (ML) workloads require enormous amounts of both structured and unstructured data to build and train models. As data scientists experiment with models and evolve them for new business requirements, new data stores are created for testing and training. This constant movement of production data into nonproduction environments may expose it to potential exploits. Putting data at the center of your security strategy will help ensure that controls are extended to wherever data exists in the cloud—be it inside or outside of production environments.

## » 3. Microservices drive more services and granular data access

The cardinal rule of football, basketball, baseball and other ball games is to keep your eye on the ball. The same lesson applies to cloud data security: Keep your eye on the data. Doing so was easier for legacy applications, which were built with a three-tier architecture and a single data store. In that scenario, protecting application data merely required protecting that one database.

Modern app development uses multiple microservices with their own data stores that contain overlapping pieces of application data. This vastly complicates securing data, especially as new features often introduce new microservices with more data stores. The number of paths of access to these data stores also increases quadratically over time. Continuously reviewing the security posture of these multiplying data stores and access paths by hand is impossible—and is one more reason for using automation to help keep the team's eye on the data.

# Data Explosion in the Cloud-Native Era


Excessive access to data for modeling
AI & ML
Explosion in # of deploys, frequency of changes
Explosion in number of services, granularity of access
Data proliferation
CICD
Cloud native app development
Move to Iaa5 + infrastructure as code
Privacy regulations
Multiple regulatory requirements
Diverse data stores, multiple copies of data
Easy to misconfigured cloud resources - data stores, IAM policies, compute

## 4. Data proliferation brings more copies into more places

The proliferation of copies of data in different cloud storage locations is a big issue for organizations using infrastructure as a service and infrastructure as code options. These architectures allow getting things done quickly, but "faster" often means there's no one looking over your shoulder to apply security checks to the expanding data. Putting data at the forefront of your security policy will help provide the ability to automatically follow data to wherever it's stored and automatically apply security controls to ensure the data is protected from unauthorized access.

## 5. Reliance on a cloud infrastructure suffers when data access is misconfigured

Access authorization is a pillar of data security. Obviously, if there's no access authorization in place, the data is a sitting duck for attackers. But what if authorization controls are improperly implemented? Did someone simplify or remove them to facilitate easy use by DevOps? Are controls consistently applied to data wherever it resides in the cloud? Most cloud breaches are due to the misconfiguration of the cloud infrastructure (IaaS and PaaS), according to Gartner analysts. A data-first approach to security should ensure that access configurations for cloud data are properly used wherever data resides.

## 6. Privacy regulations require more control and tracking of data

Compliance is a significant driver of cloud data security. Examples include personally identifiable data for GDPR, payment account data and sensitive authentication data for PCI DSS and personal health data for HIPAA. Noncompliance in protecting sensitive data like these can trigger substantial penalties. A data-first security policy should enable automatic discovery and classification of all protected data anywhere it resides in the cloud environment.

Data is your organization's most valuable asset. As more data and workloads move into the cloud, it's imperative for security teams to have 100% visibility into where sensitive data resides and to ensure it's protected. Using a legacy castle and moat approach to security will fall short in modern environments. For the reasons mentioned, adopting a data-first strategy for security is important for keeping data secure anywhere in the cloud. And that's the purpose of DSPM.

# Normalyze customer case study: Corelight

**Industry:** Information Technology
**Business Name:** Corelight, Inc.
**Employees:** 200

## Business Problem

Corelight required more visibility into its cloud data and cloud environment risk posture to help the team better protect those assets, and to improve detection and response to potential anomalies.

## Solution

With the Normalyze Cloud Platform, the Corelight security team can now continuously discover sensitive information, determine relevant attack paths, and automate the necessary remediation efforts to secure the data. The solution also enables compliance by detecting personally identifiable information (PII) and data that falls under regulatory mandates.

## Why Corelight chose Normalyze

- Normalyze assessments instantly identify sensitive structured and unstructured data
- The platform's context-aware data security insights drive better security decision making
- Normalyze Graph determines relevant attack paths that place data at risk

> "Normalyze's data-centric vision mirrored my long-term data security vision perfectly. That vision is to have comprehensive situational and structural awareness, specifically context about how that awareness supports better security decision making."
>
> **– Bernard Brantley, CISO, Corelight**

# Normalyze customer case study: Netskope

**Industry:** Cloud Security
**Business Name:** Netskope
**Employees:** 1,500

## Business Problem

Netskope sought to improve its attack surface management program – but also needed the ability to identify sensitive, regulated, and at-risk data. Doing so would help the Netskope security team to swiftly secure critical data and maintain a stronger security posture.

## Why Netskope chose Normalyze

- Normalyze assessments instantly identify sensitive structured and unstructured data
- The platform's context-aware data security insights drive better security decision making

## Solution

With the Normalyze Cloud Platform Graph, Netskope continuously discovers sensitive data, identifies relevant attack paths, and can automate the necessary remediation efforts to secure and protect its data.

> "We often find sensitive data where we didn't expect it. Normalyze enables us to see our threats and the risk to our data with a perspective we just didn't have before."
>
> **– John Knotsyphom, Threat and Vulnerability Assessment Manager, Netskope**

# How to get started with DSPM

**Getting ready to start a DSPM platform trial is simple, particularly if the provider is using an agentless model for its solution.** You'll need the following:

- Identify existing cloud provider(s) … AWS, Azure, GCP, etc.
- Gather cloud account details, such as Account ID, nickname, etc.)
- Authorized user(s), such as name, title, email address, and other details needed for people who will operate the DSPM trial and Proof of Concept.

Typically, you will enter this information into the DSPM provider's account signup form. The trial team should consider gathering a known inventory of data stores in the organization's cloud infrastructure prior to the trial. The inventory will provide a benchmark to compare what you think you know about the organization's data to what DSPM discovers is really out there. Prepare to be surprised!

# Sign up for a DSPM platform demo

**We encourage you to start your investigation of DSPM by trying a live platform in your own environment.** 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.

**For a free trial of the Normalyze DSPM platform, please visit the Normalyze website at**
https://normalyze.ai

**or** click here to get a hands-on demo.

Data-first cloud security

Normalyze™

data-first cloud security

normalyze.ai