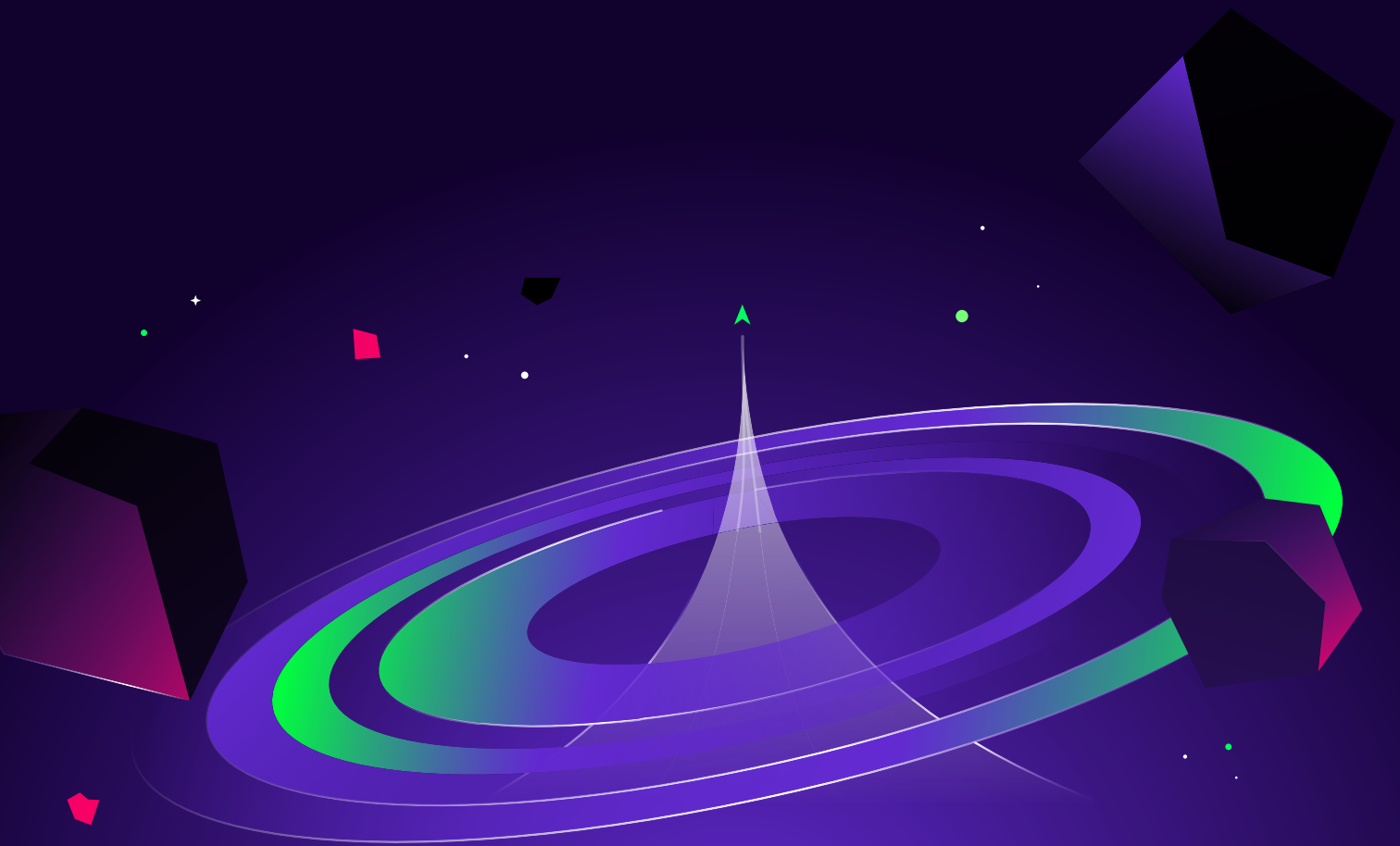
CYERA

GUIDE

DSPM Buyer's Guide

How to Evaluate DSPM Technologies

Table of Contents



Data Security Challenges in the Cloud Era

We have entered an era of unprecedented data growth and utilization. With cloud resources available at our fingertips, data is just as easily created as it is shared. Organizations have embarked on cloud migration projects, pulled by the allure of scalability, flexibility, and enhanced collaboration. Along with the benefits of the cloud, there are new and daunting challenges: volumes of data to oversee, new threats to stay ahead of, and regulatory complexities to navigate.

84% of security leaders indicate that improving zero trust security posture is a top priority.[1]

By embracing hybrid environments, we enable greater data democratization yet acknowledge the widening of the data attack surface. We must shift our strategy to **adopt a zero trust framework,** ensuring that data regardless of location – on-premise or cloud – is secure and available to only those who need it.

To do this, we as security leaders and practitioners must maintain visibility of data, manage user access to data, and enforce strong security and privacy controls. Data Security Posture Management (DSPM) and Data Detection and Response (DDR) are innovative technologies that provide security teams with that visibility and control.

89% of security leaders indicate that the data security status quo at their company is a problem.

39% of security leaders indicate that legacy technologies are insufficient for current requirements.

DSPM and DDR are emerging technologies that many vendors claim to offer. However, the lack of sufficient analyst research and customer testimonials around these technologies makes them hard to evaluate.

This guide provides a framework for security leaders to evaluate DSPM and DDR technologies, based on the challenges you are looking to address.

[1] Forrester Research Report: Automate Cloud Data Security and Risk Insight for Modern Business Resiliency

The DSPM Checklist

Consider the following requirements in a DSPM solution:

- ○ Deploys in minutes without the need for agents, overhead, and continual maintenance.
- ○ Scans structured and unstructured data.
- ○ Identifies data across IaaS, PaaS/DBaaS, SaaS environments and on-prem.
- ○ Uses AI to autonomously classify sensitive data with 95%+ accuracy.
- ○ Uses AI to learn and classify an organization's unique data and objects.
- ○ Contextualizes data so you know what the data represents and its risks.
- ○ Continuously scans the data for changes including newly created, removed, and modified data.
- ○ Automates data risk assessments that include security, privacy and other compliance exposures from data storage, datastore configurations, and data access.
- ○ Highlights data exposures and vulnerabilities related to missing backups, compliance violations, overly permissive access, and more.
- ○ Maps risks to popular regulatory frameworks like GDPR, CCPA, HIPAA, PCI DSS, GLBA, HITECH, NIST, and SOX.
- ○ Continually assesses risks to data, enabling you to quickly eliminate sensitive data exposures and threats.
- ○ Dynamically monitors where data is created or changed or when processes expose sensitive data to new risks.
- ○ Identifies when changes to data and access create security and privacy exposures.
- ○ Correlates events into prioritized alerts that accurately determine the risk associated with the issue.
- ○ Provides toolchain integrations with actionable remediation guidance to reduce mean-time-to-respond.

Key Questions Security Teams Must Answer

What is exposing my business to risk?

Automation is key to identifying security and privacy exposure as data is being created, consumed, and used across an enterprise's data landscape.

Data is constantly being generated, duplicated, and moved. As a result, it is scattered throughout an organization's data landscape, and it's not always clear where sensitive data is located, who can access it, or what exposes the business to risk.

81%

are prioritizing real-time exposure detection, data security posture management, and automated data risk assessments.

What data do I have?

In hybrid environments, a cloud-native architecture is required to keep pace with the evolution and sprawl of data.

Modern businesses use 5 or more tools to manage their data security posture. That is because traditional data security tools are siloed to structured or unstructured data, certain deployment models, or specific use cases. The discovery capabilities they bundle have had limited success and are hard to manage in cloud environments.

47%

say manual processes are too cumbersome.

42%

say implementing data security technologies takes too long.

Where is my data managed?

As of 2023, 60% of all corporate data is stored in the cloud. The average enterprise uses 1,295 cloud services, which requires a cloud-native architecture to continuously discover datastores and sensitive data as data evolves.[2]

Security teams strive to understand their data, but inventories are typically based on sanctioned datastores from a single point in time. This makes the gap between the data a business manages and how it's understood widen over time. That's because data changes and evolves.

66%

struggle to identify security exposures.

74%

estimate that their organization's sensitive data was breached at least once in 2022.

[2] https://www.zippia.com/advice/cloud-adoption-statistics/

Who can access it?

The average employee uses 36 cloud-based services every day. With over 200 collaboration applications in frequent use, sensitive data proliferates widely and is frequently shared beyond the scope of data governance policies, risking misuse or exposure from compromised accounts.[3]

To become data-driven, users must have access to data. But doing so increases your exposure. Organizations need a mature information governance program to drive awareness and standards for managing data and enforcing appropriate access controls.

74%

say that improving their ability to enforce least privilege access is critical.

64%

agreed that DSPM will improve insider threat detection and response.

How can I take action to remediate exposures?

Context, coupled with toolchain integrations, is necessary for security teams to close the gap on mean-time-to-respond when it comes to issues that matter most.

Legacy data security approaches focus on patterns and tags which causes security teams to be inundated with security alerts they can't trust. Not knowing if risks are real leads to fatigue and wasted time figuring out where to focus.

10%

is the expected accuracy rate of some traditional data classification tools.[4]

43%

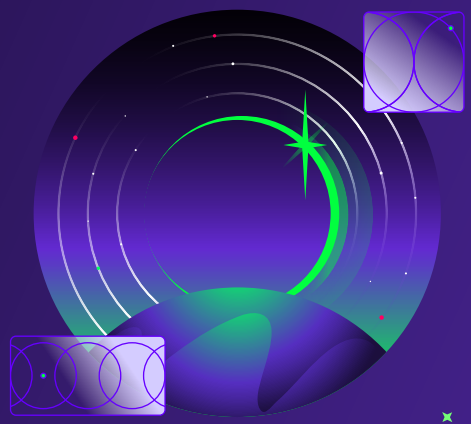
of cloud security alerts are false positives.[5]

65%

struggle to enable controls to protect data.

[3] https://www.zippia.com/advice/cloud-adoption-statistics/
[4] Nightfall AI: What's the difference between Regex and AI-based Detection?
[5] Orca 2022 Cloud Security Alert Fatigue Report

How to Spot a Legacy Approach Claiming DSPM



Slow deployment

Legacy data security technologies attempt to provide visibility into an organization's data, but the process of deploying is slow, taking months and years. Most of the process is manual and human initiated. Since these technologies must be pointed at specific datastores to initiate scanning, teams must first align on the datastores in scope to be discovered. In addition, there can be separate architectures for data depending on where it's located, adding further complexity just to connect. This starts with a proof of concept (POC) – **if a vendor cannot deploy a POC in hours to days, this is an indication that your deployment will take months or years to achieve.**

Lack of scalability

Legacy data security technologies seek to scan large volumes of data, but run into performance issues, taking days or longer for a single datastore. Some tools attempt to circumvent this by placing stringent limits on how much data is scanned within each datastore. This method yields inconclusive results in high volume datastores or datastores with diverse and complex data. This is reflected in the time it takes to produce a datastore inventory and initial data classification. **In a POC, this process should provide initial visibility within 24 hours and take at most two weeks.**

Static visibility

Legacy data security technologies are designed only to capture data from one point in time. Unfortunately, visibility constructed from dated snapshots provides an inaccurate picture of data because data, its environment, and the context that determines the risk of data are always changing. **This is a topic that you should raise and plan to evaluate during the POC process before you purchase.**

Inaccurate classifications

Data classification from legacy data security technologies yield inaccurate outputs, largely as a result of it being a human-managed process. Most classification processes rely on regular expressions (RegEx) to identify patterns in the data and determine its classification. While RegEx is a useful technique to label data, it requires validation. Either the manual validation process occurs, significantly slowing down the process, or the validation portion is skipped, resulting in outputs that cannot be trusted. **Ask your vendors to explain how classification is performed and develop a plan to verify classification accuracy across environments, deployment models, and structured and unstructured data to ensure that precision (accuracy) and recall (consistency) are high.**

Key Considerations for a DSPM Solution

To improve your data security posture in light of increased data volumes and complexity, these are the key capabilities and questions to consider:

Data discovery and classification

Cyera's DSPM solution continuously identifies the location of data and its significance, giving security teams a holistic view of their sensitive data landscape and data security posture.

What to look for	Why it matters	Questions to ask
Cloud-native architecture	Provides quick and agentless deployment.	• Does the solution use cloud-native APIs to quickly connect to datastores? • Can the solution discover the 'unknown unknowns' across your data landscape?
Continuous data discovery	Automatically detects changes to an environment without the need for manual, or 'human initiated' action.	• Can the solution detect changes to your data? • Does the solution provide a holistic view of the data?
AI-powered data classification	Uses a mix of machine learning and large language models (LLMs) for high precision and recall accuracy.	• How confident are you in the solutions ability to deliver fast results and precise outputs?
Data contextualization	Automatically detects changes to an environment without the need for manual, or 'human initiated' action.	• Does the solution tell you the residency of the data? • Does the solution tell you the security controls applied to data, whether it's encrypted or in plaintext?

Automated data risk assessment

Cyera's DSPM solution highlights data exposures, vulnerabilities, and other issues that compromise an organization's sensitive data, allowing you to take appropriate actions to harden your security posture.

What to look for	Why it matters	Questions to ask
Holistic sensitive data inventory	Provides a list of an organization's data with details such as the datastores, data classifications, number of records, and data context.	• Are you confident that the solution can deliver an accurate data inventory? • Does the solution continuously scan and catalog data, capturing data changes to maintain an up-to-date view?
Risks mapped to regulations	Identifies risk factors and connects them to specific regulatory frameworks and controls.	• Does the solution evaluate your data security posture against security, privacy, and regulatory frameworks?

Operational resilience and preparedness

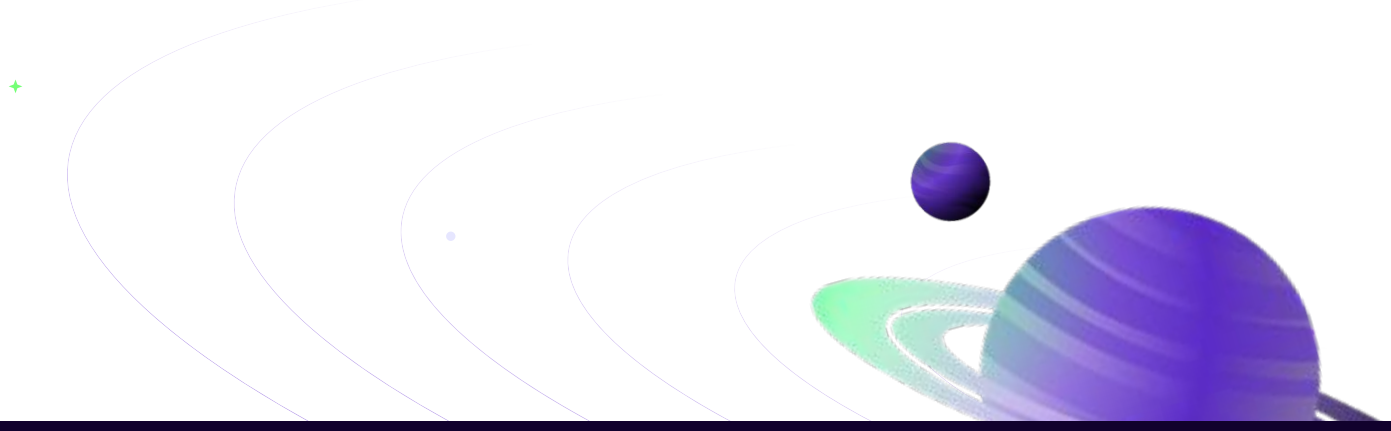
Cyera helps organizations harden their data security posture so that disruptions to data systems are averted and security teams are seen as enablers of the business.

What to look for	Why it matters	Questions to ask
Strong policies	Describes the issues that expose sensitive data or signal a direct violation of a regulation.	• Does the solution include policies that address your data risks, risk tolerance, and applicable regulations?
Resilient posture	Prepares your organization against threats to the data.	• Does the solution enable you to close the gap on data vulnerabilities?
Adaptable controls and enforcement	Applies appropriate controls and safeguards, given the state of data.	• Can the solution tell you when credentials data is exposed?

Cloud-native data security posture management

Cyera provides the ability to proactively reduce the attack surface by identifying data exposures in advance with its DSPM solution, as well as to defend against attacks in real-time with its data detection and response capabilities.

What to look for	Why it matters	Questions to ask
Broad coverage	Achieves visibility of sensitive data and its exposures, wherever the data or issues reside across the enterprise data landscape.	• Does the solution provide a unified view of data and its exposures, at rest and in use? • Does the solution cover my business-critical datastores (provide a list)? • Does the solution detect datastores added or removed without human interaction?
Real-time data detection and response (DDR)	Detects and remediates data exposure-related events as they happen.	• Does the solution flag data exposures, configuration changes, non-sanctioned data access, and data exfiltration in real time?
Contextualized alerts	Tells the story behind an event so that you can determine its risk and prioritize the most urgent issues.	• Does the solution provide context so that you can prioritize the issues that matter most?
Integrated remediation workflows	Streamlines issues management with integration across multiple tools.	• Does the solution help you resolve alerts quickly by integrating workflows with IT ticketing systems, SOAR, and SIEM tools?



Cyera is the Leading DSPM Solution

Cyera takes a data-centric approach to security, assessing the exposure to your data at rest and in use and applying multiple layers of defense.

Because Cyera applies deep data context holistically across your data landscape, we are the only solution that can empower security teams to know where their data is, what exposes it to risk, and take immediate action to remediate exposures and assure compliance without disrupting the business.

Learn why Cyera is the leading data security posture management solution by scheduling a demo today.

Get Started

About Cyera

Cyera is the data security company that gives businesses deep context on their data, applying proper, continuous controls to assure cyber-resilience and compliance. Cyera takes a data-centric approach to security across your data landscape, empowering security teams to know where their data is, what exposes it to risk, and take immediate action to remediate exposures. Backed by leading investors, including Sequoia, Accel, Cyberstarts and Redpoint Ventures, Cyera is redefining how companies secure data in the cloud.
To learn more, visit www.cyera.io

Trusted by

LifeLabs · ACV · Cboe · Mercury Financial · Veolia · Cystic Fibrosis Foundation · Advance · UTA