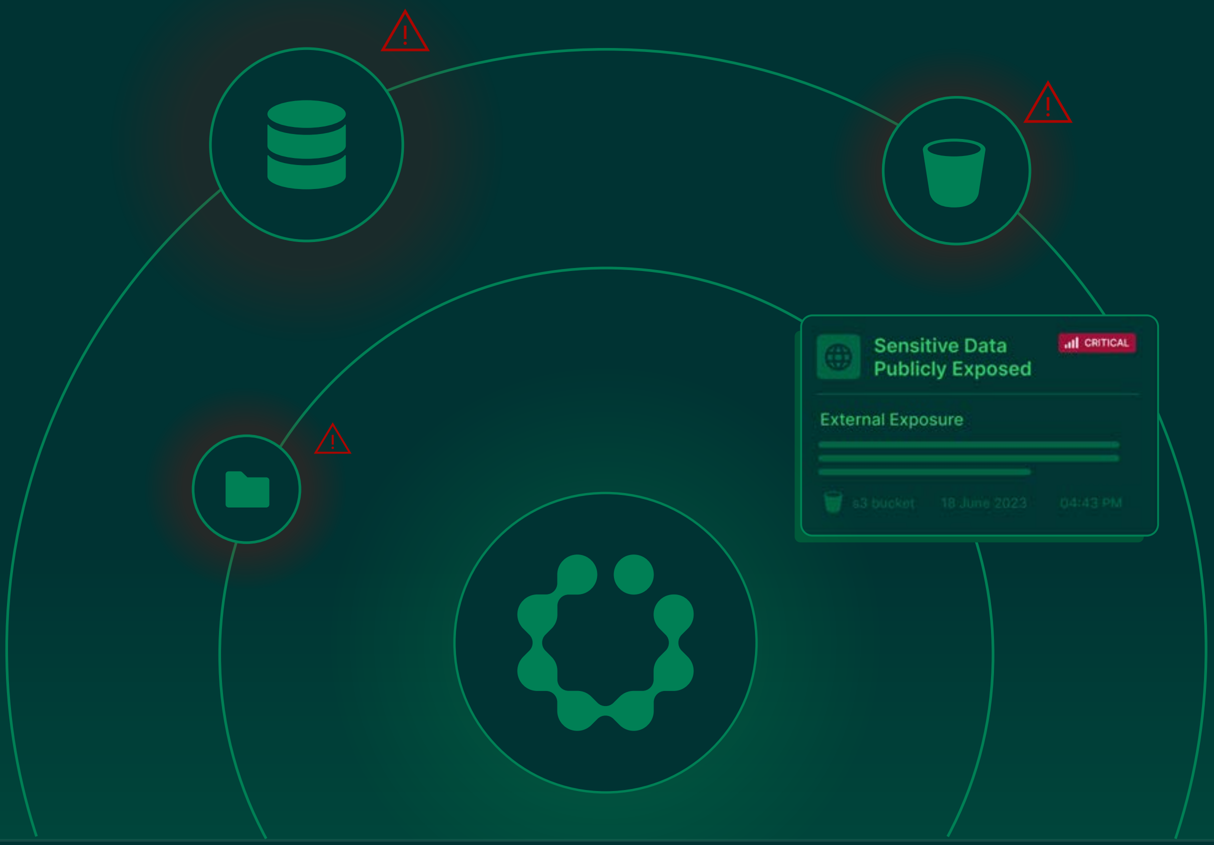
CYERA

Top 10 DSPM Requirements

Data Security Challenges in the Cloud Era



www.cyera.io | info@cyera.io

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. This raises the question: do organizations have full control and visibility of their data and are able to properly manage and secure it.

Considering that most organizations store their data in the cloud and on-premises, the data attack surface continues to widen. We must shift our strategy to adopt a zero-trust framework, ensuring that data, regardless of location — cloud or on-premise — is controlled and secured and, most importantly, available to only those who need it.

To achieve this goal, security leaders and practitioners must guarantee and maintain the visibility of data, manage user access to data, and enforce strong security and privacy controls. For this reason, Data Security Posture Management (DSPM) is the foundation of any organization's data security activities. It is a comprehensive approach designed to enhance the visibility and security of an organization's data across all environments. DSPM involves continuously identifying, classifying, and protecting sensitive data, irrespective of its location—whether in multi or hybrid cloud environments or on-premises.

The DSPM Checklist

10 requirements to consider in a DSPM solution:

- □ Scans structured and unstructured data 01
- □ Identifies data across IaaS, PaaS/DBaaS, SaaS and on-premises environments 02
- □ Uses AI to autonomously classify sensitive data with 95%+ accuracy 03
- □ Uses AI to learn and classify an organization's unique data and objects 04
- □ Contextualizes data so you know what the data represents and its risks 05
- □ Dynamically monitors when processes or changes to data and access expose sensitive data to new risks 06
- □ Continuously scans the data for changes: newly created, removed, and modified data 07
- □ Automates data risk assessments that include security, privacy, and other compliance exposures from data storage, datastore configurations, and data access 08
- □ Highlights data exposures and vulnerabilities related to missing backups, compliance violations, overly permissive access, and more 09
- □ Provides toolchain integrations with actionable remediation guidance to reduce mean-time-to-respond 10

How to Spot a Legacy Approach Claiming DSPM

Recognizing legacy approaches that claim to be a DSPM solution is important to avoid inefficiencies, scalability issues, and inaccuracies in data security management.
It also helps adopt a more effective, modern approach that aligns with current data protection needs and compliance requirements.

Issues	Legacy Approach	Ideal Proof of Concept (POC)
Slow Deployment	Legacy technologies take months to deploy due to manual and human-initiated processes. Additionally, there can be separate architectures for data depending on where it's located, adding further complexity just to connect.	A POC should deploy in hours to a few days, indicating quicker deployment capabilities than legacy systems which take months to deploy.
Lack of Scalability	There are performance issues and limits on data scanned that lead to inconclusive results. This is reflected in the time it takes to produce a datastore inventory and initial data classification.	In a POC, data scanning should provide initial visibility within 24 hours and comprehensive results in at most two weeks.
Static Visibility	Only captures data from one point in time, providing outdated snapshots.	Plan to evaluate changing data and environments during the POC process before purchasing a solution. The environment and the context should be the key factors that determine the risk of data - which is always changing.
Inaccurate Classifications	Relies on human-managed processes and regular expressions (RegEx), resulting in unreliable and inaccurate outputs.	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.

Cyera's Approach to Advanced Data Security

Unlike legacy DSPM solutions, Cyera helps organizations improve data security visibility, posture, and control, especially in complex and high-data volume environments. Cyera's modern approach to data security and DSPM specifically consists of:

Data Discovery and Classification

Cyera continuously identifies the location of data and its significance, giving security teams a holistic view of their sensitive data landscape and data security posture. Our DSPM solution is built on a cloud-native architecture that allows for quick and agentless deployment and leverages cloud-native APIs for efficient data discovery.

Automated Data Risk Assessment

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

Operational Resilience and Preparedness

Cyera describes the issues that expose sensitive data or signal a direct violation of regulation so that disruptions to data systems are noticed; we help security teams be seen as enablers of the business.

Cloud-native Data Security Posture Management

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

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 more at www.cyera.io or follow Cyera on LinkedIn.

Trusted By

Paramount LifeLabs ACV Cboe VEOLIA MERCURY FINANCIAL UTA ADVANCE