

DSPM BUYER'S GUIDE



INTRODUCTION

The growing list of high-profile data breaches shows that traditional perimeter-focused security can't address the data security challenges we face in a cloud-first era. Very little data lives on endpoints, which serve primarily as gateways to where critical data really lives — in complex hybrid cloud environments.

Most enterprises use dozens of collaboration apps like Microsoft 365, Google Workspace, and Salesforce — all of which house mission-critical data. Add hybrid NAS devices, on-prem file shares, AWS, Azure, and GCP, and **it's easy to see why enterprises have lost visibility into where their sensitive data lives, who has access, and whether it's under attack.**

ENTER DSPM



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 stored or application is.

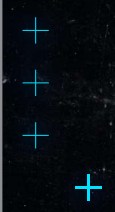
GARTNER

Although DSPM is a new acronym, data discovery, data access control, and data monitoring are not new concepts. However, the emergence of DSPM as a product category has helped bring much-deserved attention to data security at a time when data sprawl, complexity, and risk are at an all-time high.

We designed this guide to help you understand the different types of DSPM solutions, avoid common pitfalls, and ask questions to ensure you purchase a data security solution that meets your unique requirements.



THREE EVALUATION TIPS FROM CISOS



We asked three CISOs for their No. 1 tip when considering a DSPM vendor.

1. Run a proof-of-concept (POC).

“My golden rule when evaluating any new technology is to validate claims with a POC. Vendors who refuse to do a POC should raise red flags. Try to do POCs on production systems or sandboxes that mimic your production environment’s scale. For DSPM, test data classification results for false positives.”

2. Ask for a sample risk assessment.

“Ask to see an anonymized risk report from a real customer — not a marketing brochure. This can help you understand if the vendor offers the level of granularity and depth you’re after. Sample reports can help you determine if a POC is worthwhile.”

3. Read real customer reviews.

“Be careful judging vendors based on awards and press, many of which are pay-to-play. Look for [validated DSPM reviews](#) from trusted sources like Gartner and Forrester. Ask to speak directly to reference customers. Make sure they have customer case studies on their website. You don’t want to be their first big customer.”

NOT ALL SOLUTIONS ARE CREATED EQUAL.

Many vendors are trying to ride the DSPM wave. The market is full of solutions advertised as DSPMs but don't actually improve your data security posture or help stop data breaches.

Here are a few passive DSPM-like solutions to look out for:



Discovery-only DSPM

Vendors with roots in data privacy and governance are masquerading as DSPMs. They lack the context needed to identify whether sensitive data is at risk, resulting in non-actionable information. These products measure data security posture by counting sensitive data findings and do not consider exposure levels, fix issues, nor detect threats to data. Discovery-only DSPMs are essentially data catalogs.



IaaS-only DSPM

Many DSPM vendors focus on the big three IaaS platforms (AWS, Azure, and GCP) but ignore other critical data domains like cloud file storage, on-prem file shares, SaaS apps, and email. While databases and buckets in multi-cloud environments are crucial to secure, look for a DSPM vendor that [spans all your data domains](#) so you can have unified visibility and apply consistent policies across the board.



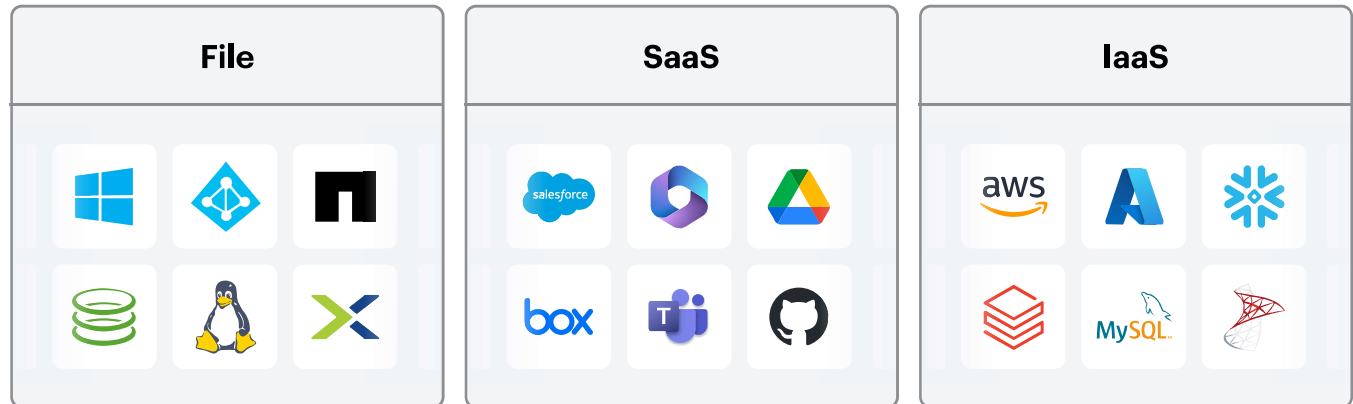
DSPM vendors without cybersecurity expertise

Just as you'd expect your EDR/XDR vendor to have strong threat intelligence and research capabilities, your data security vendors should have [research teams](#) focused on finding vulnerabilities, tracking threat actors, and developing new threat models.

TOP FIVE THINGS TO LOOK FOR IN A DSPM

1. COVERAGE ACROSS ALL DATA DOMAINS & DATA TYPES

Most large organizations store critical data in three big domains:



Buying a DSPM that only covers a single domain would be like purchasing an EDR that only worked for Macs. It might be impossible to find a single DSPM that covers every single data store your business uses. Instead, follow the 80/20 rule. **Ask yourself where your most mission-critical data lives and prioritize those data stores.**

VARONIS PROTECTS ENTERPRISE DATA WHERE IT LIVES.

Varonis covers structured, unstructured, and semi-structured data across all three domains. Our platform also maps and monitors attack paths that provide access to data, including directory services (Active Directory, Okta, and Entra ID); network traffic from proxy servers, VPNs, DNS, and firewalls; and API/OAuth connections.

Browse all our coverage →

2. ACCURATE & SCALABLE DATA CLASSIFICATION

Data discovery and classification are a foundational element of DSPM. However, many classification projects fail because the scanning engine can't process large data sets or they produce too many false positives to be trusted. Look for a DSPM with customers that match your size and scale. During your POC, ensure their classification can produce complete, contextual, and current results.

01/ Is your data classification complete?

Does your DSPM scan all your data, or is it over-reliant on sampling or “predictive” scanning?

Sampling can be effective for databases but doesn't work for large file stores like NAS arrays or object stores like S3 and Azure Blob. Unlike a database, you can't assume that just because you scanned 2TB of an S3 account and found no sensitive content, the other 500TB of data is not sensitive.

02/ Does your data classification have context?

Once you find sensitive data, what happens next? Is the data exposed? Is it being used? Who is the data owner?

Most organizations are surprised at the number of sensitive files and records they find — and the list will be different tomorrow and the next day. If your DSPM does not map permissions or track access activity, it's virtually impossible to action the finding.

03/ Is your data classification current?

Does your DSPM scan and classify data as it is created and modified?

If your DSPM does not keep a real-time audit trail of data activity, its classification engine must check the last modified date on every single object to know whether it must be re-scanned or perform a full re-scan at specific intervals (usually monthly or quarterly).

29,648 events on sensitive data		18 alerted events	1,719 events by admin accounts	
Platform	Event type	Object name	Is sensitive?	Account type
	file modified	HOW_TO_DECRYPT.txt		Admin
	share link created	Bonus.xlsx		Executive
	file deleted	Product_SKUs.pptx		User
	client DNS request	mega.co.nz		Admin
	authentication	corp.local		Service account

VARONIS' DATA CLASSIFICATION IS COMPLETE

We scan multi-petabyte customer environments top-to-bottom and put sensitivity in context with permissions and activity. Varonis classification results are always current because our activity auditing detects files created or changed; there is no need to re-scan every file or check the last modified date.



3. DEEP ANALYSIS BEYOND DATA CLASSIFICATION

What does it mean to truly “cover” a platform?

Many DSPM vendors will check the coverage box for any platform they can connect to, regardless of whether they provide actual DSPM capabilities. Some vendors will even purport to cover a data store, but in reality, they simply provide you with a developer SDK, and you have to build your own connector.

DSPM must go beyond answering whether a file or object is sensitive, taking into account whether data is at risk of a breach, and answering questions like:

- + Is our data being used? By whom? Are there any abnormal access patterns that could indicate compromise?
- + Is our sensitive data labeled correctly so that our downstream DLP controls work?
- + Is sensitive data exposed publicly? To all employees? To people who don't require access?
- + Is our sensitive data stored in unsanctioned repositories? Are we in violation of any data residency requirements?
- + What is the likelihood that a compromised user could exfiltrate sensitive data?
- + What data is stale and can be archived or deleted?

Here's a helpful scorecard of eight critical DSPM ingredients and two bonus questions you can provide vendors to better understand the depth of their coverage for each platform:

DSPM ingredient	AWS	Salesforce	Data store XYZ
Data sensitivity	Yes	Yes	
Resource inventory (objects, files, folders, users)	Yes	Yes	
Sensitivity labels	Yes	N/A	
Effective permissions	Yes	Yes	
System configurations	Yes	Yes	
Entitlements	Yes	Yes	
Third-party apps & API connections	No	Yes	
Audit trail of events	Yes	Yes	
Can you commit changes to the platform?	Yes	Yes	
Is the connector written by the vendor in-house?	Yes	Yes	

Entitlements vs. effective permissions

One of the most critical data security questions is: who can access sensitive data?

This question is not always easy to answer. In fact, calculating true effective permissions for a user in real-time can be computationally challenging and goes far beyond simply reporting on a user’s entitlements. This task is especially difficult for platforms like Microsoft 365 and Salesforce, which have obscenely complex permissions models.

Entitlements are permissions or rights assigned to a user, group, or entity. They are the figurative keys on a key ring.

Effective permissions represent a user or entity's permissions for a resource. They take into account the cumulative effect of all entitlements and access control settings, including inheritance, muting permissions, group memberships, explicit grants, global access, and other dynamic factors. They are the figurative doors that the keys unlock.

Your DSPM’s ability to visualize effective permissions is absolutely critical for breach investigations, compliance audits, and other data security use cases. This visualization is impossible without building specialized connectors for each data store and application.

Comparing **Barak Cohen** to **Josh Hammond**

Josh Hammond

Details System Permissions Code Access Object Access Field Access

Permission name	Barak Cohen	Josh Hammond
> Special data permissions	(0/1) ✖	(1/1) ✔
> Community settings	(2/2) ✔	(0/2) ✖
> Marketing cloud	(0/1) ✖	(1/1) ✔
> Platform setting controls	(0/3) ✖	(3/3) ✔
> Reports and dashboards	(1/1) ✔	(0/1) ✖
> Sales cloud	(0/2) ✖	(2/2) ✔

VARONIS GOES WIDE AND DEEP.

Varonis collects all eight ingredients from most of the platforms we monitor. We have over 150 patents, many of which relate to combining metadata to help answer critical data security questions such as, “Which data is sensitive, overexposed, and stale?” or “What sensitive data can a user access across our entire environment?”

Our unique metadata analysis also allows us to automate remediation at scale. For example, because we know whether permissions are being used or not, we can easily revoke excessive permissions with the assurance that no business process will break.

4. AUTOMATED REMEDIATION

CISOs don't need another product to tell them they have problems without offering an automated way to fix them. Look for a DSPM solution that goes beyond visibility and automates fixes on the data platforms it's monitoring.

When a vendor says they offer automated remediation, ask:

- + Do you commit changes to the target platform to remediate the risk?
- + What are the specific data risks that you can remediate automatically?
- + Can you simulate the change before committing?
- + Can you automate remediation natively, or does it require clicking a button or executing a homegrown script?

Security Posture

[Open \(4,124\)](#) [Closed \(15\)](#)

Case	Assignee	Severity	Data Source	Status
➤ Password detected in Confluence	Zara Thornfield	Critical	Confluence	Open
➤ Password on SMB share	Felix Moonshadow	Critical	SMB	Open
➤ External access to PII	Aria Sterling	Critical	AWS	Open
➤ External access to GDPR	Caspian Frost	Critical	AWS	Open
➤ Unencrypted AWS database	Luna Evergreen	Critical	AWS	Open

Often, vendors will claim automated remediation when they simply open a ServiceNow ticket (often called a "finding" or a "case") for a human data owner to investigate, fix, and close manually.

Policies

Name	Category	Event type	State
Remove collaboration links	Remediation	remove collaboration links	☒ Enabled
Remove links	Remediation	remove collaboration links	☐ Disabled
Remove stale collaboration links	Remediation	remove stale collaboration links	☒ Enabled
Remove stale group memberships	Remediation	remove collaboration links	☐ Disabled
Remove stale permissions	Remediation	remove stale permissions	☐ Disabled

VARONIS CONTINUOUSLY & AUTOMATICALLY REMIEDIATES DATA SECURITY RISKS.

Eliminate risky permissions, misconfigurations, ghost users, sharing links, and more without manual effort. Varonis comes with ready-made remediation policies that you can personalize for your organization.

5. REAL-TIME BEHAVIORAL ALERTS & INCIDENT RESPONSE

Data is the target of almost every cyberattack and insider threat.

Finding sensitive data and ensuring that only the right people have access are essential to maintaining a strong data security posture. However, DSPM must also be able to monitor data access, alert you to abnormal behavior, and stop threats in real time. As we mentioned earlier, it's a red flag if your DSPM vendor does not have an incident response function and a cybersecurity research team that regularly publishes data-centric threat research.

Look for a DSPM vendor that incorporates data detection and response (DDR) and can achieve the following:



Log all actions on data, not just alerts.

During an investigation, you want a full searchable forensics audit trail inside your DSPM. You don't want to have to jump into your SIEM or come up empty when asked to see all actions on a specific data set.



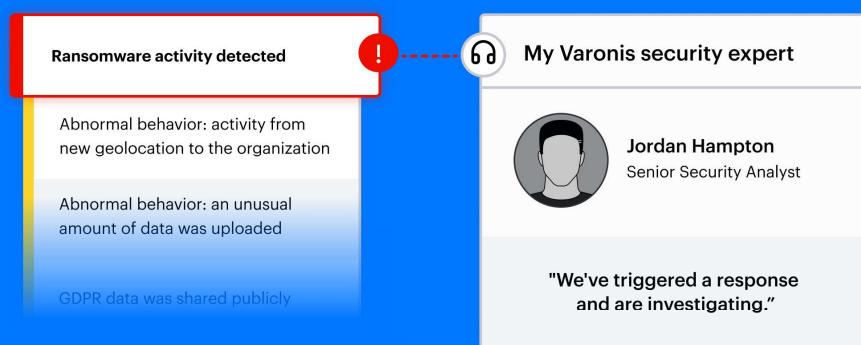
Alert you to behavior anomalies.

If your DSPM only has static rule-based alerts (e.g., alert when a user modifies more than 100 files in under a minute), you run the risk of missing stealthy attacks and insider threats. Find a DSPM with data-centric user and entity behavior analysis (UEBA) capabilities.



Help you respond to incidents.

Does your DSPM vendor have a team that can help you investigate an incident? At a minimum, can their alerts be sent to your SIEM, SOC, or SOAR so that your own incident response team can respond to threats to sensitive data?



VARONIS STOPS DATA BREACHES.

Varonis monitors data activity in real time, giving you a complete, searchable audit trail of events across your cloud and on-prem data. Hundreds of expert-built threat models automatically detect anomalies, alerting you to unusual file access activity, email send/receive actions, permissions changes, geo-hopping, and much more. Varonis also offers Managed Data Detection and Response (MDDR).

YOUR DATA. OUR MISSION.

We hope this guide helps you in your quest to find a DSPM vendor that can drive the outcomes you're looking for! If you have any questions, don't hesitate to [contact us](#).

Partner with the leader in data security.

Gartner

#1 DSPM vendor
on Garner Insights

FORRESTER

Leader in Forrester Wave™:
Data Security Platforms,
Q1 2023

GIGAOM

Leader in GigaOm Radar
for Data Security Platforms
(DSPs)

Reduce your risk without taking any.

Our free Data Risk Assessment takes minutes to set up and delivers immediate value. In less than 24 hours, you'll have a risk-based view of the data that matters most and a clear path to automated data security.

Get a demo at www.varonis.com/demo.



About Varonis

Varonis (Nasdaq: VRNS) is a leader in data security, fighting a different battle than conventional cybersecurity companies. Our cloud-native Data Security Platform continuously discovers and classifies critical data, removes exposures, and detects advanced threats with AI-powered automation.

Thousands of organizations worldwide trust Varonis to defend their data wherever it lives — across SaaS, IaaS, and hybrid cloud environments. Customers use Varonis to automate a wide range of security outcomes, including data security posture management (DSPM), data classification, data access governance (DAG), data detection and response (DDR), data loss prevention (DLP), and insider risk management.

