eBook

Five Things to Consider when Choosing a DSPM Solution

thalestct.com

THALES
Building a future we can all trust

Contents

Introduction

The modern enterprise has become a sprawling ecosystem of cloud services, data lakes, third-party integrations, and AI-infused applications. With this complexity comes a new reality: sensitive data is everywhere, including places it shouldn't be.

Traditional security tools are ill-equipped to handle dispersed, dynamic environments:

- Perimeter defenses fail to account for cloud-based assets.
- Manual classification systems can't keep up with the velocity and volume of data generation.

With increasing regulatory pressure and a surge in high-profile data breaches, organizations face a sobering truth: they don't know where all their sensitive data is, who's using it, or whether it's adequately protected.

Some organizations are turning to **Data Security Posture Management (DSPM)**—a new class of security technology that offers the visibility and control enterprises need to protect their most valuable digital assets. However, like any powerful tool, DSPM must be deployed with care and consideration. This eBook answers the foundational question of where to start with DSPM by looking at five critical questions every organization must answer before investing in a DSPM solution. It aims to help organizations determine how to make the right decisions for their data, their people, and their risk profile.

What is Driving DSPM Adoption?

As organizations in every industry face new and evolving challenges in data security, several key trends are driving the adoption of DSPM solutions. These trends align with broader shifts in technology, regulations, and market needs. In addition, many organizations face resource constraints; they do not have the workforce required to perform manual tasks and understand their risk environment. All these factors make it clear why Data Security Posture Management is becoming an essential solution for enterprises.

The Evolving Regulatory Landscape

As data privacy and protection regulations continue to evolve and tighten, entities are under growing pressure to maintain compliance. Regulations require organizations to maintain a strong posture around data discovery, access controls, data classification, and risk identification—all key components of DSPM. Failing to meet these compliance standards can land a organization in hot water, resulting in hefty fines, loss of customer trust, legal wrangles, and operational setbacks.

A Lack of Visibility

Digital environments are sprawling, meaning visibility across the data lifecycle is more critical—and more challenging—than ever. Data lives everywhere now: in cloud environments, on-premises systems, SaaS platforms, and data lakes. Yet, most organizations struggle to keep track of where sensitive data resides or how it is being accessed and shared.

According to the Cloud Security Alliance report Understanding Data Security Risk 2025, nearly a third (31%) of respondents do not even have the right tools to identify their riskiest data sources. Add in the ease with which data can be copied or shared without proper controls, and the risk of exposure increases dramatically—especially when sensitive information ends up in unknown or external locations.

Data Risk Sprawl

The rapid expansion of data across on-premises, hybrid, and multi-cloud environments has led to a phenomenon known as "data sprawl," where sensitive information becomes fragmented and difficult to manage. This sprawl encompasses structured, semi-structured, and unstructured data types, including emails, documents, and social media posts, scattered across various systems and locations.

Over half of the CSA Data Security Risk 2025 respondents reported operating in hybrid environments, while 27% use multi-cloud setups. The fragmented risk profiles and data distribution inherent in these cloud platforms make it harder to locate and prioritize vulnerabilities and can result in inconsistent management practices. As a result, Concentric AI reports that 83% of organizations acknowledge visibility gaps in their data security posture, directly weakening their defences. These challenges underscore the necessity for DSPM solutions, which provide up-to-the-minute visibility, automated classification, and monitoring to mitigate risks associated with data sprawl.

AI Enables More Sophisticated Attacks

AI is also adding fuel to the fire. Generative AI tools enable threat actors to launch more convincing, scalable phishing attacks that are increasingly difficult to detect. Research backs this up—a recent report from Sapio and Deep Instinct found that 75% of security pros have seen an uptick in attacks, with 85% attributing it to bad actors using GenAI. While MFA is a foundational defense, it is no longer enough. Modern security strategies must also incorporate behavioral monitoring, such as detecting logins at odd hours or from unusual geographies, to catch subtle anomalies that could indicate compromise.

The Quantum Threat

While today's challenges are daunting, tomorrow's might be even more so. Quantum computing is on the horizon and poses a serious risk to current encryption methods. Chips like Microsoft's Majorana 1 signal a near future where algorithms like RSA and ECC could be cracked. The Thales 2024 Data Threat Report warns that "harvest now, decrypt later" attacks—where encrypted data is stolen today and decrypted when quantum becomes viable—are already happening. Organizations need to prepare now, adopting quantum-resistant encryption and building crypto agility into their security programs.

Insider Risks

But not all threats are external. Insider risks—whether intentional or accidental—remain a persistent danger. The 2024 Thales Data Threat Report shows that security leaders are just as concerned about internal exposure as they are about external breaches. Traditional perimeter security is not enough. Organizations must continuously monitor behavior, access patterns, and anomalies to detect and mitigate insider threats in real time.

To stay ahead of these trends and threats, entities must move from reactive defense to proactive risk detection, tackling vulnerabilities before they turn into incidents.

5 Questions to Guide Your DSPM Selection

1. Where is My Sensitive Data?

For many organizations, the most perilous data isn't what's securely stored—it's the data they're unaware of possessing. This includes outdated databases forgotten on legacy servers, unstructured files adrift in public cloud folders, and data duplicated across various platforms without proper oversight. These blind spots, often termed "shadow data," are unclassified, unmonitored, and unmanaged, posing significant security risks.

The complexity intensifies in today's enterprise environments, where sensitive data sprawls across on-premises servers, hybrid clouds, and a multitude of SaaS applications. This dispersion creates numerous hiding places for critical data, increasing the likelihood of it slipping through the cracks.

The volume of data is relentless. Organizations generate vast amounts daily—from structured CRM databases to the chaotic realm of emails, contracts, and collaborative documents. Tracking the real-time location of all this data is a formidable challenge without the right tools.

Compounding the issue, data is in constant motion—copied, transferred, shared, and accessed by various systems and users. Pinpointing a specific file or data point at any given moment, especially across hybrid environments, is no small feat.

Alarmingly, 35% of data breaches in 2024 involved shadow data—unmanaged and unclassified information outside of IT's purview. These breaches took 26.2% longer to identify and 20.2% longer to contain, with an average cost of $5.27 million, underscoring the severe financial impact of unmanaged data.

This underscores the non-negotiable need for visibility. Enterprises must implement automated data discovery and classification tools that continuously scan for sensitive data, regardless of where it resides. These tools not only help identify known data but also uncover hidden shadow data, ensuring comprehensive data governance.

Only by automating this process can organizations keep pace with the rapid creation, movement, and transformation of data, ensuring sensitive information is classified correctly, protected, and accounted for.

Because in data security, what you don't know can—and will—hurt you.

What to look for in a DSPM solution

When evaluating a Data Security Posture Management (DSPM) solution, look for features that ensure effective data protection.

Feature	Description
Automatic Data Discovery	Automatically discover and catalog all data stores across multi-cloud, hybrid, and on-prem environments
AI/ML-Driven Classification	Use AI and ML to accurately classify sensitive data like PII, PCI, IP, and more
Continuous Scanning	Support ongoing scanning to detect new, modified, or moved data
Support for Diverse Formats	Manage data in various formats supporting both structured and unstructured data seamlessly

2. Who Has Access to My Sensitive Data?

It is one of the most uncomfortable truths in cybersecurity: many organizations simply do not know who has access to their most sensitive data. Not because they are negligent, but because the tools they rely on cannot keep up with the complexity of modern enterprise systems.

Security teams are left in the dark without a unified way to collect and analyze access data across various platforms—on-premises, in the cloud, and everywhere in between. In this darkness, risks multiply, and sensitive data can become accessible to far more people than intended, and no one may realize it until it is too late.

The root of the problem is that access control in today's enterprise is far from straightforward. It is a maze of role-based access control (RBAC), attribute-based access control (ABAC), custom permissions, and legacy rules layered on top of each other over the years of growth. The result is a web of permissions that even the most seasoned IT teams struggle to untangle.

There is also the human factor to consider. In large firms, different departments often operate like self-contained islands, managing their own IT stacks with their own rules. This kind of decentralization breeds inconsistency, making it impossible to paint a complete, real-time picture of who has access to what.

The consequences are more than theoretical. A single over-provisioned account—or one forgotten user with lingering privileges—could provide a perfect opening for an attacker or lead to accidental data exposure. And without clear insight into access rights, detecting and responding to these risks becomes a guessing game.

To regain control, organizations must start with visibility. That means scanning data store locations for granted user rights and mapping those privileges directly to database objects across all systems. It's not just about knowing who is accessing what—it is about knowing who can and under what circumstances.

Understanding your true data access posture is not a one-time audit—it is an ongoing process that requires automation, consistency, and, above all, clarity.

When access is left unchecked, not just your data is at risk—it is your entire organization.

What to look for in a DSPM solution

When evaluating a DSPM solution, look for the following features.

Feature	Description
Identity-to-Data Mapping	Map who (or what) has access, how it is granted, and audit trails for changes
Alerts on Excessive Privileges & External Access	Flag risky access like over-privileged users or third parties
Least Privilege Recommendations	Suggestions to reduce access to only what is necessary, with automation support to streamline enforcement

3. How Well Are Credentials Protected?

While encryption is a cornerstone of data protection, it's only as effective as the mechanisms controlling access to the encrypted data. This brings into focus two critical components: credentials and access rights.

Credentials—comprising usernames, passwords, API keys, and cryptographic certificates—serve as the digital identity of users and systems. They authenticate entities attempting to access systems. However, authentication alone doesn't dictate what actions an authenticated entity can perform. That's where access rights come into play, defining the specific data and operations that an authenticated user can perform, such as viewing, editing, moving, or deleting.

The distinction is crucial: possessing valid credentials doesn't inherently grant unrestricted access. Yet breaches often exploit this nuance. According to the Verizon 2025 DBIR, 22% of initial access malicious actions were due to compromised credentials, while 31% of internal actor breaches were due to privilege abuse.

The challenge grows exponentially in cloud-first environments. Most enterprises now work with multiple cloud service providers (CSPs), each with their approach to key creation, management, and rotation. What begins as a well-intentioned move toward data protection quickly spirals into a tangle of inconsistent policies, varying protection levels, and rising operational costs.

Different departments may deploy their data security solution for encryption independently, sometimes even for the same types of data, resulting in fragmented oversight and a higher risk of key and access mismanagement. Without clear visibility and centralized control, organizations face a real threat: unauthorized access, data loss, or compliance violations that stem not from a lack of encryption but from poor key hygiene.

A unified encryption key and secrets management system can bring order to chaos. Enterprises can dramatically improve their security posture by consolidating key generation, storage, rotation, backup, recovery, revocation, and termination into a single platform.

More importantly, centralization enforces a critical security principle: separation of duties. When the person managing encryption keys cannot access the encrypted data—and vice versa—it creates a natural check-and-balance system that limits insider risk and ensures compliance with best practices.

In the end, encryption is not just about locking up your data—it is about ensuring the keys are stored far away from the lock in a place only the right people can reach. Even the strongest lock is useless if the wrong hands hold the key.

What to look for in a DSPM solution

When evaluating a DSPM solution, look for the following features.

Feature	Description
Exposed Secrets Detection	Scan code, logs, and data stores for exposed secrets like API keys and passwords, triggering alerts when found
Credential Auditing	Assess rotation frequency, expiration, and MFA enforcement
Reuse Identification	Pinpoint which accounts, applications, and APIs access sensitive data
Non-Human Identity Monitoring	Identify bots and automation tools and flag excessive or outdated permissions

4. How Has My Sensitive Data Been Used?

Most organizations think they know how their data is being used; however, in reality, many are flying blind. Without advanced monitoring and logging tools in place—and more importantly, fully integrated—gaps in visibility are all but guaranteed. And in those blind spots, risk thrives.

Modern enterprises do not operate in neat, contained environments. Data lives everywhere—on-premises servers, multiple cloud platforms, SaaS applications, and the growing constellation of employee devices. Each environment has its own quirks and ways of handling data, making it incredibly difficult to get a unified view of how information is accessed, shared, or modified.

This goes beyond an operational challenge—it is a regulatory minefield. Frameworks like GDPR, HIPAA, and others require organizations to maintain detailed logs of how sensitive data is handled. But when data flows across departments, platforms, and borders, compliance can quickly become overwhelming.

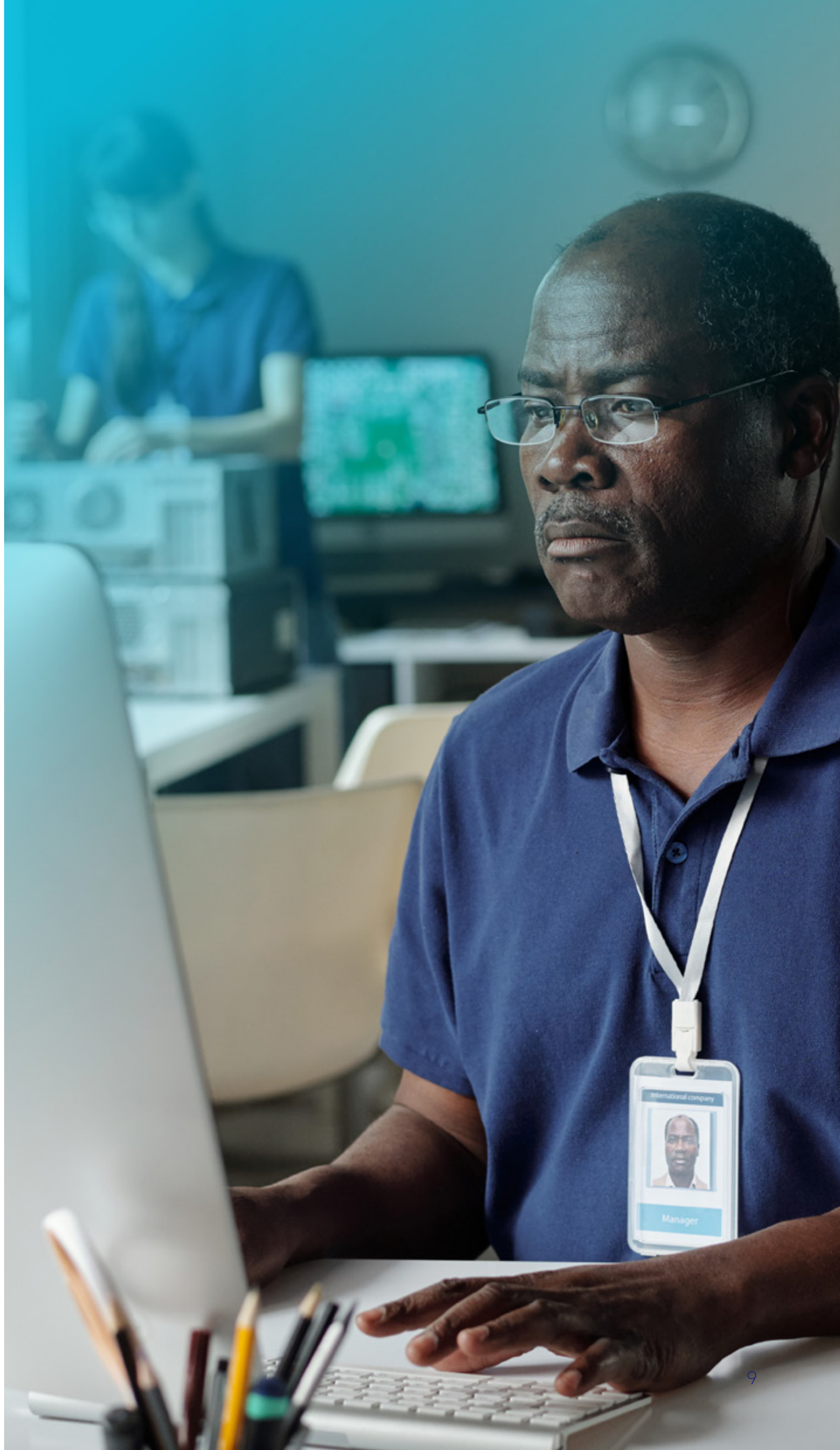
To stay ahead, organizations need more than logs—they need intelligence. Effective data usage tracking requires automated, real-time visibility into where data lives, who is accessing it, and how it is being used. It is about building a full picture, not just collecting fragments.

This is where data-centric compliance and security tools are proving so effective. By automating workflows and surfacing recommended actions, they empower security teams to spot vulnerabilities before they escalate. They cut through the noise, highlight suspicious behavior, and support proactive risk mitigation—not just reactive clean-up.

What to look for in a DSPM solution

When evaluating a DSPM solution, look for the following features.

Feature	Description
Track Data Access Events	Correlate activity with users, roles, and endpoints
Highlight Anomalies	Detect patterns like mass downloads or unusual access times
Support Forensics	Provide audit trails and visual timelines for investigations
Connect to Business Context	Differentiate between legitimate workflows and potential misuse to reduce false positives and prioritize real threats



5. What Is the Security Posture of My Data Stores?

When defending sensitive data, posture management is a continuously evolving defense strategy. Doing it well requires more than a static checklist; it calls for real-time intelligence, continuous monitoring, and regularly updated vulnerability insights that evolve as fast as the threats they aim to stop.

A key component is scanning, not the occasional sweep, but ongoing, automated scans powered by up-to-date vulnerability definitions. These scans assess everything from databases to servers, flagging known weaknesses and gauging the level of exposure using trusted industry benchmarks.

At the heart of effective risk management is prioritization. Organizations today must not only identify vulnerabilities but also assess their severity and determine which ones demand urgent attention. While frameworks like the Common Vulnerability Scoring System (CVSS) have historically provided a standardized method for evaluating risk, many organizations, including leading DSPM solutions, adopt customizable scoring systems tailored to their unique data environments and priorities.

The goal remains the same: to provide a consistent and actionable way to measure risk, understand potential impacts, and ensure that security teams focus first on the exposures that could cause the greatest harm. Much like a Richter scale for cybersecurity, these scoring models help translate complex risk signals into explicit, prioritized action.

Posture management cannot end with scans, either. Monitoring plays a critical role, too. The always-on radar delivers real-time insight into what is happening across data environments—from system events and alerts to gateway health, agent status, violations, file access, and more.

With so many moving parts, not all alerts are created equally. Some are harmless, while others may be signs that a breach is happening. The key is tuning systems to distinguish between the two. By leveraging pre-configured severity ratings or building custom policies, organizations can filter out the noise and zero in on what matters.

Ultimately, effective posture management is about staying a step ahead. It is about knowing not just where your organization is vulnerable but how and why—and being ready to act before attackers exploit the opening.

What to look for in a DSPM solution

When evaluating a DSPM solution, look for the following features.

Feature	Description
Continuous Scanning	Detect configuration drift, misconfigurations, and policy violations across cloud and on-prem environments
Security Standard Enforcement	Ensure that encryption, tokenization, and access controls are in place and properly configured
Support Forensics	Map posture to frameworks like NIST, ISO 27001, and CIS to stay audit-ready
Prioritized Remediation	Gain clear, ranked guidance to fix high-risk issues first, saving time and reducing exposure

How Thales Can Help: Secure Your Data with Confidence

Sensitive data is distributed across clouds, on-premises, and hybrid environments, so achieving comprehensive security and compliance requires more than just visibility—it needs actionable protection strategies. Thales is uniquely positioned to support organizations on their Data Security Posture Management (DSPM) journeys, providing solutions that give them the necessary visibility and integrate advanced data protection, encryption, tokenization, and access control.

At the heart of the Thales offering is CipherTrust Data Security Posture Management, a powerful and flexible solution that allows organizations to safeguard their data and maintain compliance across increasingly complex environments.

Thales solution promises six key differentiators

Prioritize Security Measures Based on Data Risk Assessments

Thales CipherTrust DSPM empowers organizations to prioritize security measures based on comprehensive data risk assessments. Leveraging advanced analytics and customizable risk scoring evaluates factors such as data sensitivity, user access patterns, and encryption strength across diverse environments. This holistic approach enables security teams to identify high-risk data assets and allocate resources effectively, promptly addressing the most critical vulnerabilities. Thales facilitates proactive mitigation strategies that align with organizational priorities and compliance requirements by focusing on data-centric risk indicators.

Classify Data Based on Sensitivity and Value While Assessing Risk

In addition to risk assessment, Thales excels in classifying data based on its sensitivity and value. CipherTrust DSPM provides complete visibility into the location of sensitive data across an enterprise, enabling organizations to uncover and close compliance gaps. This granular classification allows for tailored security policies and encryption strategies, ensuring that high-value data receives appropriate protection. By aligning data classification with objectives, Thales enables organizations to manage data security effectively, reduce exposure to threats, and maintain regulatory compliance.

Comprehensive Encryption & Key Management

Thales delivers robust encryption and key management capabilities through CipherTrust DSPM, which secures data and metadata. Whether a company's data is stored in the cloud, on-premises, or in hybrid environments, CipherTrust DSPM ensures that sensitive data is encrypted and protected, even should a breach happen.

Centralized key and secrets management allows entities to securely manage encryption keys and secrets across their full infrastructure, tightly governing control and access. In the event of a breach, the encrypted data remains unreadable without access to the correct decryption keys, mitigating the risk of exposure.

Identification of AI-related Data Risks

Thales DSPM solution distinguishes itself by proactively identifying AI-related risks, particularly those stemming from "shadow AI" services—unauthorized AI tools adopted without IT oversight. These services can inadvertently lead to data leakage through unmonitored AI queries. Thales addresses this by continuously monitoring for abnormal behaviours, such as an influx of AI-generated requests or commands that may indicate system probing or reconnaissance activities. By leveraging advanced analytics and machine learning, Thales' DSPM provides visibility into AI interactions, enabling organizations to detect and mitigate potential threats before they escalate.

Quantum-Ready Protection

As the quantum menace looms large, Thales is ahead of the curve in preparing organizations for the post-quantum era. CipherTrust provides quantum-safe encryption by offering support for post-quantum cryptographic algorithms, helping organizations prepare for the inevitable challenges quantum computing will bring.

With CipherTrust, organizations can future-proof their cryptographic strategy and see that they are protected against quantum-based threats. The platform also offers a quantum-ready key management framework, which supports the seamless integration of quantum-safe algorithms, providing a scalable and secure approach to cryptographic transition.

Context-Aware Incident Response

CipherTrust Data Security Posture Management also offers context-aware incident response. Tracking and correlating data access events across systems gives entities deep visibility into what happened as well as why it matters. This level of visibility helps security teams quickly identify anomalies, such as unusual access patterns or potential insider threats, and respond to them in real-time before they become a problem.

CipherTrust also enables organizations to see the full scope of data access and usage across the enterprise, featuring audit trails and forensics capabilities that aid incident investigation, and provide critical insights into data activities. This helps firms prioritize responses and maintain compliance with regulatory bodies and requirements.

Are you ready to see how Thales can help protect what matters most—your sensitive data?

Explore how the CipherTrust Data Security Posture Management delivers end-to-end protection, supports compliance goals, and prepares organizations for the challenges of AI and quantum-era threats.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

THALES

Building a future we can all trust

Contact us

For office location and contact information,
please visit thalestct.com/contact-us

thalestct.com