

DSPM Readiness Checklist for MSPs & MSSPs

Are you ready to deliver scalable, data-first security services?

What is DSPM anyway?

Data Security Posture Management (DSPM) is a rapidly emerging cybersecurity category first identified by Gartner in its 2022 Hype Cycle for Data Security. As described by Gartner, 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.**”

Why DSPM matters

Traditional security models focus on securing infrastructure—servers, endpoints, or networks—rather than the data itself. Yet today's hybrid and cloud-native environments demand a data-first approach. DSPM flips the model, placing the data asset at the center of detection, risk assessment, and remediation.

DSPM technology helps service providers proactively identify, prioritize, and mitigate data exposure risks across cloud, on-prem, and hybrid environments.

How to Use This Checklist

For each question, assign yourself a score based on your current capabilities:

2

✓ **Yes:** We have this in place

1

⚠ **Somewhat:** We're working on it or it's partially implemented

0

✗ **No:** We do not have this capability

Visibility & Discovery

Can you automatically discover all assets and endpoints (on-prem, cloud, remote)?



Do you have continuous visibility into where sensitive and regulated data lives?



Can you identify shadow IT or unmanaged data repositories in client environments?



Risk Prioritization & Context

Are you able to classify data by sensitivity (e.g., PII, PHI, PCI)?



Do you have a method to prioritize exposures based on business impact, not just vulnerabilities?



Can you correlate data risk with user access, asset type, and location?



Operational Efficiency

Is your DSPM solution multi-tenant and designed for MSSP delivery?



Does it integrate easily with your existing SIEM, SOAR, and ticketing platforms?



Can your analysts and service teams operate it without specialized training?



Compliance Support

Does your solution map data risks to regulatory frameworks (GDPR, HIPAA, CCPA, etc.)?



Can you generate audit-ready reports and evidence for client compliance reviews?



Can your platform support privacy and governance teams with actionable insights?



Client Value & Reporting

Can you provide clients with clear, executive-friendly dashboards showing risk reduction?



Do you offer recurring assessments or DSPM-as-a-Service packages?



Are you able to demonstrate service value in terms of data protection and compliance outcomes?



Cost & Resource Alignment

Is your DSPM solution lightweight and quick to deploy (hours/days, not weeks)?






Does it help reduce tool sprawl and consolidate your security stack?



Is it priced in a way that allows you to build profitable services at scale?



Scoring & Readiness Results

Score	Readiness Level
33-36	 You're DSPM-ready! Your business is well-positioned to launch and scale high-margin, data-first services.
24-32	 You're nearly there Focus on building automation and operational efficiency into your data security stack.
< 24	 Start with the fundamentals Begin by establishing data visibility and prioritization as a foundation for DSPM.






Ready to take the next step?

Cavelo was built by a former service provider, for service providers. Its unified platform is designed to help MSPs and MSSPs like yours reduce complexity, increase visibility, and deliver high-impact, data-centric security services at scale.

Unlike traditional security tools that only focus on endpoints or vulnerabilities, Cavalo brings together asset discovery, data classification, identity access insights, vulnerability management, and configuration benchmarking into a single, easy-to-operate solution.

It's everything MSPs and MSSPs need to see, manage, and reduce data risk—without adding friction or tool sprawl.

Cavelo helps service providers:

-  **Know Where Sensitive Data Lives**
Automatically scan and classify sensitive data across Windows, Mac, Linux, and cloud environments. Identify shadow data and blind spots across all client environments—so nothing is missed.
-  **Prioritize What Really Matters**
Correlate data value with known vulnerabilities and exposure context. Go beyond generic alerts to deliver risk-based prioritization that aligns with business impact.
-  **Eliminate Device and Data Blind Spots**
Continuously discover and monitor all devices and assets across client networks, including unmanaged or rogue endpoints.
-  **Understand Who Has Access and Why It Matters**
Instantly view identity and access history—across people and AI agents. Spot risky permissions, shared file activity, and inappropriate access to sensitive data. Don't just monitor risk — manage it with Cavelo.
-  **Validate System Hardening and Security Posture**
Benchmark client environments against CIS, Microsoft, and other best practices. Identify misconfigurations and weaknesses before they become exposures.

Lead with insight.
Protect with confidence.

Take a self-guided tour to see how Cavelo can bring your business and service delivery to the next level.

Take the Tour