



Cavelo for MSPs & MSSPs:

A Modern Approach to Data-Centric Security

*How to Deliver Scalable, Profitable,
and Differentiated Services with Turnkey DSPM*

How to Use This Guide

This guide is designed for Managed Security Service Providers (MSSPs), Managed Service Providers (MSPs), cybersecurity leaders, and technical service teams looking to expand their offerings, reduce operational complexity, and deliver measurable, data-first security outcomes to their clients.

As cyber threats grow more evasive and compliance demands intensify, service providers are under increasing pressure to do more—with less. At the same time, clients are asking harder questions about data risk, regulatory exposure, and the true business value of their security investments. This guide will help you navigate that shift.

What You'll Find Inside:

1

A breakdown of the most pressing challenges service providers face today

2

An overview of Data Security Posture Management (DSPM) and how it supports modern service delivery

3

A look at how Cavelo aligns DSPM capabilities to service provider priorities

Whether you're building new services, evaluating tools, or trying to differentiate in a crowded market, this guide will help you assess where you are—and where you can go—with turnkey DSPM capabilities and a platform like Cavelo.

Start with the challenges, consider your current capabilities and then explore how Cavelo can help you unlock new value and scalability with data-first security.

How to Use It:

- ✔ Service planning and roadmap development
- ✔ Technology consolidation and stack evaluation
- ✔ Go-to-market strategy for data risk, compliance, and exposure management offerings
- ✔ Client-facing conversations around data visibility, governance, and breach prevention

The MSP & MSSP Challenge Landscape

Service providers play a critical role in protecting today's complex, hybrid IT environments. But with rising expectations, changing threats, and economic pressure, providers are grappling with a new wave of challenges:

Tool Sprawl and Integration Complexity

MSPs and MSSPs are juggling too many tools that don't talk to each other. [65% of IT and security pros](#) say they use too many security tools, and over half say those tools lack integration, which impairs detection and delays threat response.

The average organization uses [83 security tools from 29 vendors](#), costing up to 5% of annual revenue in overhead and inefficiencies.

Difficulty Demonstrating Business-Aligned Value

Clients demand proof of impact. Service providers must go beyond alerts to provide meaningful, data-driven insights tied to risk reduction, compliance, and outcomes.

Organizations adopting platformized security see [4x better ROI](#) and significant reductions in vendor management and training costs.

Resource Constraints and Talent Shortages

Tool complexity, alert fatigue, and onboarding delays strain already stretched service provider teams.

[96% of MSPs say security services improve client retention](#), highlighting the growing importance of delivering measurable, strategic value.

Pressure to Reduce Total Cost of Ownership (TCO)

Consolidation isn't just a buzzword—it's a business necessity. Service providers must reduce licensing overhead, simplify operations, and cut TCO without sacrificing service quality.

74% of security leaders say attackers accessed sensitive data during breaches, and 86% of those organizations paid ransom—underscoring the cost of [poor visibility](#).

Limited Visibility into Client Data Risk & Exposure

Many MSPs and MSSPs struggle to understand where sensitive data resides, how it's exposed, and whether it's protected—especially in shadow IT, SaaS, and hybrid environments.

60% of MSSP professionals [report burnout](#), with 78% saying they lack time to upskill or manage new tools.

Client Demands for Compliance and Privacy Support

With rising regulatory requirements like GDPR, CCPA, HIPAA, and NIS2, clients expect service providers to help manage data compliance and minimize liability.

Compliance is now one of the [top drivers of MSSP growth](#), especially in regulated industries.

What is DSPM?

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 technologies automate and centralize:

- ✓ Discovery and classification of sensitive data across cloud and on prem
- ✓ Risk assessments based on data sensitivity, location, and access
- ✓ Guided remediation workflows and compliance monitoring

How DSPM Works

DSPM tools generally follow this lifecycle:

- 1 Data Discovery & Classification:**
Continuously scan structured and unstructured data stores—including shadow IT and SaaS—for sensitive content.
- 2 Risk Assessment & Exposure Scoring:**
Analyze who has access to data, how it's used, and evaluate its exposure risk in context.
- 3 Remediation & Continuous Monitoring:**
Surface policy violations, recommend corrective action, and enforce governance controls to prevent recurrence

DSPM vs. CSPM vs. DLP

Technology	Focus	Key Differentiator
DSPM	Directly protects sensitive data	Where data lives, who accesses it, and its security posture
CSPM	Infrastructure / Cloud misconfiguration	Securing cloud infrastructure (not data itself)
DLP	Data exfiltration control	Preventing data leaks rather than assessing exposure risks

DSPM complements CSPM and DLP by closing the visibility gap around shadow data, over-permissioned access, and data sprawl—critical gaps that are particularly problematic for MSSPs managing complex client environments.

The Role of DSPM in the Modern Security Stack

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

DSPM gives providers:

- ✓ Continuous visibility into sensitive and shadow data
- ✓ Contextual risk scoring based on sensitivity, access, and location
- ✓ Compliance and privacy mapping with audit-ready reports
- ✓ Lightweight, API-friendly integration into existing workflows

By aligning services with what clients value most (data protection and compliance) DSPM helps MSPs and MSSPs unlock new growth and deliver high-margin offerings.

Introducing Cavelo

Cavelo was built by a former service provider, for service providers.

Its unified platform is designed to help service providers like you 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, Cavelo 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 file 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.

Why a Unified Platform Matters

Service providers can't afford disjointed tools that only solve one piece of the puzzle. Cavelo delivers a fully integrated view of your client's attack surface, all tied to a unified risk score that's easy to understand.

Capability	Key Differentiator
 Data Discovery & Classification	You can't protect or assess the risk of what you can't see.
 File Permissions & Access Audit	Understand who (or what) can access sensitive data—and what's at risk if compromised.
 Vulnerability Management	Identify where your most sensitive data is most exposed.
 Configuration Management	Ensure patches and systems are securely configured from the start.
 Asset Discovery	Discover and inventory every device across the environment—no exceptions.

Built for MSPs & MSSPs from the Ground Up

- ✓ **Multi-tenant architecture** to manage multiple clients from a single interface
- ✓ **Fast deployment and agent-based discovery** across diverse environments
- ✓ **Mid-market-friendly pricing** with profitable margins for service providers
- ✓ **Intuitive interface** designed to reduce analyst workload and training overhead
- ✓ **Executive-ready reporting** to showcase your value and reduce client churn

Whether you're launching DSPM-as-a-Service or integrating DSPM into your broader offering, Cavelo provides the visibility, context, and scale you need to lead with data-first security.

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](#)