opentext™

GUIDE

From data risk to data control: The DSPM playbook

A practical guide to reducing data risk for enterprises embracing hybrid-multi cloud and AI

Contents

Why DSPM matters now

Sensitive data is increasingly distributed, duplicated, and over-retained. Traditional data security tools cannot keep up with the blind spots, regulatory exposure, and unnecessary risk that is created by the proliferation of unstructured data and the growing use of hybrid multi-cloud environments and AI. Executives need to understand where sensitive data lives, how it is exposed, and how to reduce risk without slowing the business.

This executive playbook outlines a practical, phased approach to data security posture management (DSPM), focused on visibility, prioritization, remediation, and provable, continuous improvement.

Executive value proposition

OpenText delivers a unified DSPM approach that combines enterprise-scale discovery, risk-based prioritization, automated remediation, and persistent data-centric protection—helping organizations reduce risk, strengthen compliance, and prepare for AI-driven data growth.

The DSPM journey at a glance

1. **Prepare for DSPM success:** Establish scope, align stakeholders, and set realistic expectations for a phased, low-disruption approach.
2. **Discover what you have:** Build a live data inventory: Identify and classify sensitive data, both structured and unstructured, across hybrid multi-cloud environments and SaaS applications.
3. **Understand exposure and business impact:** Correlate data sensitivity with access, usage, and business context to prioritize real risk.
4. **Fix what matters first:** Automate remediation: Reduce exposure through policy-driven remediation, data minimization, and data-centric protection.
5. **Govern access with context:** Align identity, access, and data sensitivity to enforce least privilege and prevent overexposure.
6. **Secure AI and future data workloads:** Enable safe analytics and GenAI by governing data used in training, prompts, and retrieval pipelines.
7. **Prepare for post-quantum cryptography (PQC):** Identify data requiring long-term protection and adopt a crypto-agile path to quantum-safe readiness.
8. **Monitor, measure, and improve continuously:** Track posture drift, remediation progress, and measurable risk reduction over time.
9. **Operationalize DSPM across the organization:** Embed DSPM into security, privacy, and governance workflows to sustain long-term resilience.

Executive outcomes

- Reduced breach and compliance risk
- Faster audit readiness
- Clear data risk (or DPSM) reporting for executives and boards
- Defensible data minimization
- Safer enablement of analytics and AI
- Lower storage and cloud costs

1. Prepare for DSPM success

DSPM is a phased journey. The most successful organizations start with obtaining visibility across their data estates, then expand to remediation and governance capabilities in order to mitigate risk and optimize confidence. Importantly, the effective DSPM strategy does not require perfect data hygiene to already be in place; in fact, DSPM is a critical tool to data minimization and reduction of redundant, obsolete, and trivial (ROT) data. Furthermore, it also does not require a rip-and-replace of existing tools, or a massive upfront investment.

Preparation begins by setting realistic expectations and aligning stakeholders. It is critically important that security, compliance, IT, and data teams agree on success criteria and operating principles. DSPM initiatives are most effective when they first focus on high-impact data, such as unstructured file shares, cloud object stores, and regulated data repositories, before expanding more broadly.

What to expect:

- A phased approach, rolled out incrementally by data domain or environment: Start small and expand as confidence and value grow
- Minimal operational disruption: read-only discovery; emphasis on high-impact data policy-driven actions; integration with existing security, privacy, and governance processes
- Alignment across security, privacy, IT, and data stakeholders on scope and priorities

Outcome:

A pragmatic foundation for sustainable DSPM adoption that builds momentum without overwhelming teams.

2. Discover what you have: Build a live data inventory

DSPM begins with visibility. Organizations must understand where sensitive data exists across structured databases, unstructured repositories, on-premises and cloud storage environments, and SaaS applications. Without this foundational insight, risk cannot be accurately assessed or reduced.

OpenText uses AI-assisted discovery and customizable classifiers to identify sensitive information at enterprise scale. In order to address massive data volumes and the multitude of repositories, an incremental approach must be followed. This starts by looking at metadata only, then moving to scanning of small samples of the data. When a repository is prioritized, a full scan can be performed. By correlating data sensitivity with business context—such as ownership, usage, and regulatory relevance—organizations can distinguish between theoretical findings and real risk and focus action where it delivers meaningful reduction. Discovery also reveals shadow data, duplicated content, and ROT data that unnecessarily expands the attack surface and increases cost.

What to expect:

- Automated discovery of sensitive data, both structured and unstructured, across the enterprise
- Visibility into shadow data, duplicates, and over-retained information
- Associate data sensitivity with business context to reduce the noise

Outcome:

A baseline and continuously updated inventory of sensitive data across the enterprise.

3. Understand exposure and business impact

Visibility alone is not enough. Organizations must understand how sensitive data is accessed, shared, and exposed in order to prioritize risk effectively.

DSPM provides visibility into sensitive data that can then be correlated with permissions, ownership, and usage patterns to reveal overexposure, misconfigurations, and excessive access. By combining sensitivity, access, and usage with regulatory and business context, organizations can focus on the exposures that pose the greatest real-world impact.

What to expect:

- Mapping of permissions, ownership, and usage
- Visibility into how sensitive data is accessed and used across systems and users
- Context into risk prioritized based on regulatory sensitivity and business impact

Outcome:

A risk-aware posture view focused on what matters most.

4. Fix what matters first: Policy-driven remediation

Manual remediation does not scale in modern data environments. DSPM enables a policy-driven approach to remediation at the source, allowing effort to be focused on the highest-risk exposures while minimizing disruption to business operations. OpenText DSPM helps organizations identify where risk can be safely reduced through data minimization and access cleanup, such as revoking clearly excessive or stale permissions and reducing redundant, obsolete, or trivial (ROT) data. These actions can often be automated with policy controls and approvals, delivering fast, measurable risk reduction.

Where data must be retained or risk cannot be fully addressed through deletion or access changes alone, DSPM orchestrates remediation through integration with data protection and identity systems. Encryption, tokenization, or masking can be applied based on policy, with human oversight and workflow-driven enforcement to ensure accountability and correctness. Rather than attempting to automate every action, OpenText DSPM combines automation, policy controls, and guided workflows to simplify remediation, reduce manual effort, and ensure changes are both safe and auditable.

What to expect:

- Policy-driven identification and prioritization of remediation actions based on data sensitivity and exposure
- Automated reduction of ROT and clearly excessive access where confidence is high
- Guided remediation workflows for permissions and data protection, integrated with identity and protection platforms
- Human oversight and approvals for higher-impact or irreversible actions

Outcome:

Faster, more consistent data risk reduction with significantly less manual effort—without sacrificing control or accountability.

5. Govern access with context

Once visibility and remediation are in place, access governance becomes precise rather than blunt. DSPM provides the foundational visibility and context to enable organizations to align access decisions with data sensitivity and business need.

By linking data, identity, and role context, organizations can detect toxic access combinations, enforce least privilege, and enable just-in-time access where appropriate. Furthermore, integration with behavioral monitoring and threat detection ensures that access remains appropriate as data and roles change.

What to expect:

- More precise, just-in-time and context-aware access decisions based on data sensitivity and business need
- Detection and correction of excessive or toxic access combinations
- Ongoing alignment between identity, role changes, and data risk

Outcome:

Least-privilege access aligned to business needs and data risk.

6. Secure AI workloads

AI adoption significantly expands the data attack surface and introduces new governance challenges. DSPM provides the foundation for secure-by-design AI adoption.

DSPM for AI security ensures that GenAI systems only access the data they are intended to use—and nothing more. By continuously discovering, classifying, and reducing exposure of sensitive data, OpenText delivers DSPM that limits the blast radius of prompt-injection and AI misuse, turning an unavoidable model risk into a manageable data security problem.

What to expect:

- Greater confidence in which data can safely be used for AI initiatives
- Guardrails around AI data flows, including prompts, outputs, and retrieval pipelines
- Protection for training and inference data with privacy enhancing technologies (PETs)

Outcome:

Secure-by-design AI adoption.

7. Prepare for post-quantum cryptography (PQC)

Quantum computing introduces a long-term but unavoidable shift in how sensitive data must be protected. PQC will weaken or invalidate many of today's widely used cryptographic algorithms over time, particularly those used for long-term data protection. Preparing for PQC is therefore not a future exercise; it is a data governance and risk management priority that begins today.

Effective PQC preparation starts with understanding what data truly requires long-term confidentiality. Not all sensitive data carries the same longevity, regulatory exposure, or business value. DSPM provides a critical foundation by identifying sensitive data, understanding its retention and lifecycle requirements, and helping organizations determine where stronger or future-proof cryptographic protections will be needed.

OpenText supports a measured, non-disruptive approach to PQC readiness by enabling organizations to prioritize high-value data and align with broader crypto-agility initiatives. Rather than forcing immediate algorithm changes, DSPM informs where cryptographic evolution matters most, allowing security and platform teams to plan and adapt as standards mature without breaking applications or disrupting operations.

What to expect:

- Clear visibility into sensitive data that requires long-term confidentiality
- Prioritization of data sets that warrant future quantum-resilient protection based on sensitivity, retention, and business impact
- Alignment with broader crypto-agility and platform initiatives without requiring immediate cryptographic changes

Outcome:

A clear, defensible path to post-quantum readiness that protects high-value data today while enabling smooth transition as quantum-safe standards evolve.

8. Monitor, measure, and improve continuously

DSPM is not a one-time project; it is an ongoing discipline. Continuous monitoring is essential to detect posture drift, anomalous usage, and emerging risks.

OpenText DSPM provides audit-ready dashboards and reporting that track remediation progress, risk reduction, and compliance posture over time. These insights support operational decision-making and executive reporting.

What to expect:

- Continuous visibility into posture changes, drift, and anomalous usage
- Clear metrics to track remediation progress and risk reduction over time
- Audit-ready insights that support compliance and executive reporting

Outcome:

Measurable, defensible improvement in data security posture over time, supported by continuous visibility, audit-ready reporting, and clear evidence of risk reduction for executives and regulators.

9. Operationalize DSPM across the organization

Leading organizations embed DSPM into daily operations rather than treating it as a standalone initiative. DSPM insights should inform SOC operations, identity governance, privacy workflows, and data management practices.

Clear ownership, cross-functional collaboration, and defined KPIs help ensure that DSPM becomes a sustainable business process. Over time, organizations mature from reactive cleanup to proactive, policy-driven data governance.

What to expect:

- Integration of DSPM insights into existing security, governance, and privacy workflows
- Defined ownership and KPIs to sustain progress beyond initial cleanup
- A shift from reactive data security to proactive, policy-driven governance

Outcome:

A sustainable DSPM program that adapts as data and regulations evolve.

Getting started

Organizations should begin with a focused data discovery and risk assessment to identify unknown sensitive data, quantify exposure, and establish a prioritized remediation roadmap. Starting small builds confidence, delivers early value, and creates a foundation for long-term DSPM success.

Conclusion

As data environments continue to expand and evolve, managing data risk requires more than point solutions and periodic audits. DSPM provides a continuous, scalable approach to understanding, reducing, and governing data risk across the enterprise. By following the phased journey outlined in this playbook, organizations can move from reactive data security to proactive, resilient data governance.

Take the first step toward effective DSPM by initiating a data discovery and risk assessment. Gain visibility into your sensitive data, prioritize real risk, and begin building a sustainable program that supports compliance, innovation, and long-term resilience.

Schedule a call with your OpenText representative to discuss an assessment for your enterprise.

Customer outcomes

BELBIM

Eliminated redundant sensitive data, reduced infrastructure footprint, and strengthened regulatory compliance.

Read the full customer story ›

SIX Group

Protected sensitive financial data while enabling analytics with strict access controls.

Read the full customer story ›

Major US bank

Improved compliance with Gramm Leach Bliley Act (GLBA), helping to avoid SEC fines, and strengthened brand reputation after three previous data breaches.

opentext™